TURKISH GENERAL STAFF
ANKARA

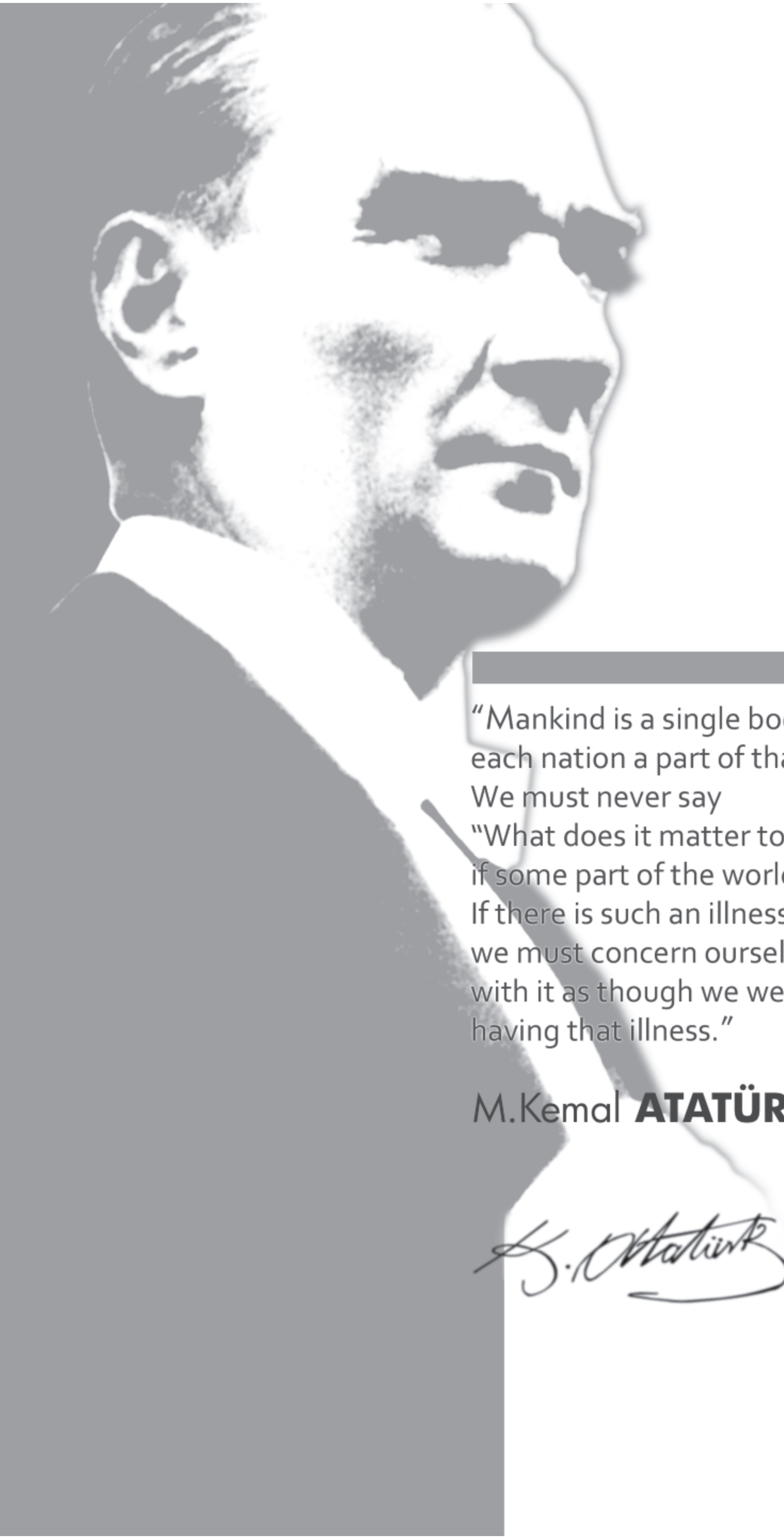
GLOBAL TERRORISM AND INTERNATIONAL COOPERATION SYMPOSIUM-III

PROCEEDINGS

15-16 March 2010
Ankara

THE TURKISH GENERAL STAFF
CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM
PUBLICATIONS

THIS PAGE IS INTENTIONALLY LEFT BLANK



"Mankind is a single body and
each nation a part of that body.
We must never say
"What does it matter to me
if some part of the world is ailing?"
If there is such an illness,
we must concern ourselves
with it as though we were
having that illness."

M.Kemal **ATATÜRK**

K. Atatürk

PROCEEDINGS
OF
GLOBAL TERRORISM AND INTERNATIONAL COOPERATION
SYMPOSIUM-III

Editor
MG Kenan KOÇAK

Board of Publication
Col. Ertuğrul Gazi ÖZKÜRKÇÜ
Col. Altan ÖZTAŞ
Ltc (TUR AF) H. Hakan KARAYEĞEN
Ms. Figen ÜNSAL

Interpreters
Cpt. (TUR N) K. Erhan ARKEŞ
Ltc (TUR AF) H. Hakan KARAYEĞEN
Maj. A. Aykut ÖNCÜ
Cpt. Behlül Bulut
Ms. Figen ÜNSAL
Ms. Zeynep SÜTALAN
Ms. Fatma DUMAN
Ms. Pınar Doğan IŞIKLAR
Ms. Egemen EGE
Ms. Nazan BERGMEN

Page Design
Cvl. Esin GAZİOĞLU

The opinions and the comments in the proceedings of “Global Terrorism and International Cooperation Symposium-III” represent the personal views of the authors. They do not represent the official views of Turkish Armed Forces. All the right of the articles and the pictures included in this book are reserved. However, they may be quoted if referred to.

CONTENTS

FIFTH SESSION THE ROLE OF INTELLIGENCE IN COUNTERING TERRORISM

CLOSING REMARKS

THIS PAGE IS INTENTIONALLY LEFT BLANK

PREFACE

LTG Mehmet ERÖZ
Chief of Operations of TGS

THIS PAGE IS INTENTIONALLY LEFT BLANK

LTG Mehmet ERÖZ

Chief of Operations of TGS

PREFACE

Sir,

Distinguished guests,

Within the scope of its annual action plan, the Centre of Excellence-Defence Against Terrorism has organised this Symposium on Global Terrorism and International Cooperation which will take place today and tomorrow.

The purpose of this widely attended symposium is to provide a platform for the exchange of experiences in the fight against terrorism in other countries, and to strengthen international cooperation in this area. This event is attended by 461 participants from 80 countries, among them NATO member countries, countries of the Partnership for Peace and the Mediterranean Dialogue, represented by ministers, chiefs of staff, and other high-ranking civilian and military officials. The event will be held in five sessions. 20 academics and high-level civilian and military officials from seven countries and from Turkey will give talks and chair the individual sessions.

The opening speech will be delivered by the Commander of Turkish Armed Forces, General İlker Başbuğ. The keynote speech will be given by Prof. Dr. Graham Allison from Harvard University, followed by General Stéphane Abrial, French Air Force, North Atlantic Treaty Organization Supreme Allied Commander Transformation.

Prof. Dr. Yonah Alexander will chair the first session in the afternoon which is dedicated to a discussion on international law in the fight against terrorism and the role of international organisations. Two presentations will be given during that session. The second session of the Symposium will be chaired by Prof. Dr. Faruk Bozoğlu. Its topic is future trends in counterterrorism.

On the second day of the symposium Prof. Dr. Tolga Yarman will chair the 3rd session on technological advances and their impact on combating terrorism. During the session two presentations will be given. The 4th session will be chaired by Mr. Ercan Çitlioğlu, and examine the role of strategic communication in countering terrorism. Three presentations will provide background information. In the afternoon session, Mr. Guy Roberts, Deputy Assistant Secretary General for Weapons of Mass Destruction Policy and Director, Nuclear Policy Planning Directorate for the North Atlantic Treaty Organization (NATO), will give a lecture on WMD Terrorism.

The 5th and final session will be chaired by Prof. Dr. Ali Karaosmanoğlu and is dedicated to the role of intelligence in combating terrorism; during the session two presentations will be given.

After the 5th session, Prof. Dr. Ersin Onulduran from Ankara University will give a general overview on the subjects addressed at the symposium. The event will be closed with a final address by General Aslan Güner, Deputy Chief of the Turkish General Staff, and the presentation of certificates to the participants.

Thank you!

OPENING REMARKS

General İlker BAŞBUĞ
Commander of the Turkish Armed Forces

KEYNOTE ADDRESS

Prof. Dr. Graham ALLISON
Harvard University

KEYNOTE ADDRESS

General Stéphane ABRIAL
Supreme Allied Commander Transformation
(SACT), NATO

THIS PAGE IS INTENTIONALLY LEFT BLANK

General İlker BAŞBUĞ

Commander of the Turkish Armed Forces

OPENING SPEECH

Distinguished Guests,

Welcome to the third “Global Terrorism and International Cooperation” symposium. I would like to express my feelings of respect and gratitude for your participation.

The developments observed and the experiences gained during the post-Cold War era have shown us how fast the global and regional security systems have changed. I think we could not have realized in a timely manner the mental transformation required for a profound analysis of these changes and producing convenient responses.

In today’s world, the likelihood of a major battle among major powers has diminished considerably. However, regional conflicts are still going on and many people are losing their lives in these conflicts.

It can be asserted that the risks and threats which emerged as security challenges especially after the collapse of the bi-polar world have assumed asymmetric rather than a symmetric nature. The greatest risks, we face today, are violence and terrorism having radical thoughts behind. Terrorism threatens the common human values, democracy, freedoms, human rights including the right to live, which are the products of centuries-long giant efforts and sacrifices. Terrorist organizations have attained the assets and the capability to launch attacks any time and anywhere in the world.

In this sense, security is also globalized in today’s world. Questioning the current security perceptions has paved the way for the emergence of new security understanding.

The term “new security” generally implies a broadening of the security perception in a way to involve a wider spectrum of threats. Apart from terrorism and military risks, these “new” threats also include the problems such as economic inequalities, injustices, environmental pollution, depletion of natural resources, ethnic conflicts, immigration, smuggling, drug trafficking and security of energy lines.

However, the “new security” is not just a matter of broadening the agenda. The broadened agenda is the result of the adoption of the new security in practice. Security is a holistic entity. From a philosophical point of view, it is an all-out renovation initiative which aims to place human needs in the locus of new security, security perceptions and implementations. This transformation in security approach reflects the adoption of a more holistic perception involving the military and all other dimensions of security.

It cannot be claimed, however, that this new human-centered security perception underestimates the security of the state. When the states nourishing and harboring terrorism in a way to pose threat for other nations are examined today, it can be seen that they are failed states having ineffective governmental agencies.

The globalized and transnational nature of terrorism necessitates international cooperation. Irrespective of its source, aim or cause, terrorism is a combination of all inhuman activities having no justification whatsoever. Yes, terrorism is inhuman and it has no mercy at all. Among our guests today, we have the Commander of the 11th Corps in Peshawar of the friendly and brotherly country of Pakistan. I had the chance to meet Lieutenant General Muhammed Masood ASLAM on 14 October 2009 during my visit to Pakistan. Unfortunately, Lt. Gen. ASLAM lost his son after a terrorist attack in Rawalpindi on 04 December 2009. I would like to express once again that our deepest sympathies are with him.

However, such events do not make us surrender to terrorism. We should keep our grief at the bottom of our heart but maintain our fight with resolve. The participation of Lt. Gen. ASLAM in this conference is a good example of this attitude. Democracy is a system of rights, liberties and responsibilities. Those who are benefiting from the opportunities provided by democracy cannot tolerate terrorist activities targeting the most basic human right, which is the right to live. Terrorism cannot be supported or ignored. At this point, I would like to underline the fact that identification of the heavenly religion of Islam with terrorism would also serve the political aim of global terrorism.

Turkey has been fighting against PKK terrorist organization for more than 30 years. Throughout this period, we had many severe casualties and it did cost a lot to us. States and nations have to be ready to pay this price when necessary, as well. From time to time we, as a nation, had to fight by ourselves. Therefore, as a result of our painful experiences, we have found out that international cooperation and fusion of power are very important issues in the fight against terrorism. It is necessary to ensure international cooperation and unity of efforts in combating terrorism.

In order to make a proper analysis of a phenomenon like terrorism, we need an interdisciplinary approach. First of all, we have to assess terrorism as a phenomenon, and then we have to understand how, where and in which conditions it emerges. We have to analyze the way of thinking of terrorism.

Another issue that has to be understood well is the relation and difference between fight against terrorism and fight against terrorist organizations or terrorists.

Fight against terrorism is a set of activities conducted comprehensively by states and in parallel and coordination with each other in the fields of security, economy and propaganda as well as in socio-cultural and international arena. These activities complement each other, however, sometimes the relationship between these activities might transform into a process of multiplication rather than addition.

When it comes to fight against terrorist organization or terrorist, this responsibility belongs to the security forces.

Now, I would like to share my views on fight against terrorism with you:

- The main objective of the fight against terrorism is to destroy the hope for success of a terrorist organization and its supporters and show them that terrorism leads nowhere. Achieving this depends on the elimination (neutralization) of the terrorist organizations.
- Fight against terrorism must be human-centered and the process must appeal to the hearts and minds of people. The following has to be ensured to attain this goal:
    - Fight against terrorism must be conducted on legal grounds.
    - In the regions that terrorist actions take place, ensuring the security of the local people is of primary importance.
    - Innocent local people must not be confused with terrorists.
    - Terrorists and those that help, encourage or sympathize with terrorists must be differentiated well and different courses of action must be developed against these people.

- In the fight against terrorism, the support of the local people for security forces must certainly be ensured.
- In fighting against terrorism, unity of effort among various organizations and agencies operating in different fields must be ensured.
- Fight against terrorism is a long-term process. We must be patient, resolved and moderated on this issue.
- We must also make it clearly understood not only by security forces but also by political decision makers, the media and the public that the fight against terrorism is a difficult process requiring patience.
- Terrorist organizations want to exhaust the patience of people by perpetuating the process. That is why they build their strategies on the societal patience. While fighting against terrorism, therefore, societal and managerial patience must be displayed.
- Again, in fight against terrorism, giving false hopes to people must be avoided.
- Terrorism is the part of the ecosystem that produces, enlivens and surrounds itself, and it coexists with it. Of course, when saying ‘ecosystem’, we mean the environment and the order we live in; the plants, animals and humans and the relations among them. The terrorist organizations try to shape the ecosystem they are in. It is important to transform the ecosystem nourishing terrorism into one that contributes to the fight against terrorism. In order to do this, proper understanding of the local ecosystem that feeds terrorism is a necessity.

In general, the ecosystems in which terrorism resides are very complex. The reason for this complexity is that the modern, post-modern and traditional networks are all intertwined.

Beside this, terrorist organizations can get involved in weapon smuggling, drug and human trafficking together with transnational crime organizations.

All these issues make it clear that fight against terrorism is a multidimensional, complex and time-consuming process. Therefore, a major aim must be to transform the ecosystem feeding terrorist organizations into a system that shortens the life of these organizations. The main objective is to create an ecosystem that isolates a terrorist organization.

Because of this, the security personnel in the field should be unified with the ecosystem in the region. They should be a part and friend of that geography.

You can only have a full control over a given geography by leaving your footprint all around. You should be an actor in ecosystem too. You should be a natural part of ecosystem for seven days, twenty-four hours.

"Interim and Voluntary Village Guards" system, which we have applied in the light of our experiences we have gained by reading the local ecosystem, has taken on important responsibilities and duties in the fight against the Separatist Terror Organization. So far the number of martyrs among Interim and Voluntary Village Guards is 1,343. That Interim and Voluntary Village Guards stand on the side of the government is a significant indication which points out that the problem is not an ethnic conflict and also that the separatist terror organization failed to get the support of the people in that region. Following the successful implementation of the village guard system in Turkey for a long time, the USA has applied a similar system (Sons of Iraq) since 2007 in Iraq. In Afghanistan too, the USA has tried to establish a local security unit or a militia force (Afghan Public Protection Force) similar to the one in Iraq and started the related pilot program in February 2009.

- Terrorist organizations have a wide spectrum of activities. The organizations can conduct different types of activities in varying degrees of density both in rural and urban areas. For this reason, it is necessary to fight against each of these using different methods.

There may appear some paradoxical cases that security forces may face during their fight against terrorism.

- Sometime disproportionate use of force as part of counter-terrorism measures may lead to emergence of even less secure circumstances.
- Sometimes disproportionate use of force may result in a decrease in success level of operations.
- Sometimes using less force and taking calculated risks may enhance the effectiveness of operation.

- Everything should be done to ensure a dynamic cooperation between security forces and intelligence organizations. It is important to collect effective, accurate and timely intelligence. Intelligence would lead the operations. Operations conducted without intelligence may yield negative results. Human intelligence collected by well-trained personnel is central to the fight against terrorism.
- Public sensitivity and the increased media control have increased the importance of not only the strategic truths but also the tactical truths. The tactical mistakes may foil proper strategic approaches. Therefore, the qualifications and competence of counter-terrorism personnel in the field act as determining factors in attaining success in this fight. It is important that the leaders in the field possess sufficient degree of sociological information

and have developed skills beyond traditional military qualifications, such as the ability to read historical and geographical facts.

- The success in counter terrorism should not be measured on the basis of the number of neutralized terrorists. A more important issue is to decrease the number of the activities initiated by terrorists.
- It is necessary to give importance to take measures to control and decrease the number of recruits and to encourage the escapes from the terror organization.
- Public determination is a factor determining success, in and by itself, in counter-terrorism.

For this reason, each layer of society and media have important duties in preventing the terror and fear which terrorists try to disseminate with the aim of forming a convenient environment for their perception management.

In our age, the individuals make use of the media in reducing this complex situation to a perceptible level. Through the media, the “reality” presents itself as “existent”, “presented” and “perceived” and it is usually presented without being examined in detail. This situation can cause serious changes on the perceptions of societies. Although freedom of the press and the neutral public information should be respected in every way, it should be kept in mind that freedoms must have their limits especially when they start damaging the society.

Exploitation of media by terrorists and terror images disseminated all over the world have an important impact on the globalization of terrorism, because the most important target of terrorists is to attract public attention to their activities, keep this attention alive and to ensure their recognition and acceptance by the system and public. Media coverage of these events especially on international TV screens is one of the purposes of their activities. In the presentation of news on terror events by media, therefore, the duration and the scope of the news and not repeating them are also important, as the repetition of terror events on national and international media for long periods of time serves the purposes of terrorist organizations.

Distinguished Guests,

During the symposium, the experts will present their observations and analyses on various aspects of terrorism, which is one of the most important and major threats to international security. I believe that this symposium will bear fruitful results in understanding the problem and in revealing what we can do together to protect our common values. I thank you all for your contributions and I wish you success.

Prof. Dr. Graham ALLISON (USA)[*]

Harvard University

Thank you very much and it is a great honour for me to be here. I just came from Boston last night and with some of the others who come from a distance we may be a little weaker than usual but it is a great pleasure to be here, I can assure you.

Who could measure, or who could have imagined? If I would have chosen a subtitle for my presentation today, it would be “Who could have imagined?” Obviously today, we live in an environment in which, as the previous speaker has said, we face conceptual challenges in addressing a national and international security context different than the Cold War context that provided the framework for most of us, for most of our professional lives. But today to try to imagine something hugely worse than any of the terrorist attacks we have seen so far,

[*] Director of Harvard's major Center for Science and International Affairs, Graham Allison has for three decades been a leading analyst of U.S. national security and defense policy with a special interest in nuclear weapons, terrorism, and decision-making. As Assistant Secretary of Defense for Policy and Plans in the first Clinton Administration, Dr. Allison received the Defense Department's highest civilian award, the Defense Medal for Distinguished Public Service, for "reshaping relations with Russia, Ukraine, Belarus, and Kazakhstan to reduce the former Soviet nuclear arsenal." This resulted in the safe return of more than 12,000 tactical nuclear weapons from the former Soviet republics and the complete elimination of more than 4,000 strategic nuclear warheads previously targeted at the United States and left in Ukraine, Kazakhstan, and Belarus when the Soviet Union disappeared. Dr. Allison’s latest book, Nuclear Terrorism: The Ultimate Preventable Catastrophe, is now in its third printing and was selected by the New York Times as one of the "100 most notable books of 2004." It presents a strategy for preventing nuclear terrorism organized under a doctrine of "Three Nos:" no loose nukes; no new nascent nukes; and no new nuclear weapons states. Dr. Allison's seminal book, Essence of Decision: Explaining the Cuban Missile Crisis, first published in 1971, and significantly revised and reissued in 1999, ranks among the bestsellers in political science with more than 400,000 copies in print. As "Founding Dean" of the modern Kennedy School, under his leadership, from 1977 to 1989, a small, undefined program grew twenty-fold to become a major professional school of public policy and government. Dr. Allison has served as Special Advisor to the Secretary of Defense under President Reagan. He has the sole distinction of having twice been awarded the Department of Defense's highest civilian award, the Distinguished Public Service Medal, first by Secretary Cap Weinberger and second by Secretary Bill Perry. He served as a member of the Defense Policy Board for Secretaries Weinberger, Carlucci, Cheney, Aspin, Perry and Cohen. Dr. Allison was the organizer of the Commission on America's National Interests (1996 and 2000) that included leading Senators and national security specialists from across the country, including former Senators Sam Nunn and Bob Graham, Senators John McCain and Pat Roberts, Condoleezza Rice, Richard Armitage, and Robert Ellsworth. Dr. Allison was a founding member of the Trilateral Commission, a Director of the Council on Foreign Relations, and has been a member of public committees and commissions, among them the Baker-Cutler DOE Task Force on Nonproliferation Programs with Russia, the IAEA’s Commission of Eminent Persons, and the Commission on Prevention of Weapons of Mass Destruction Proliferation and Terrorism. Dr. Allison has served as a Director of the Getty Oil Company, Natixis, Loomis Sayles, Hansberger, Taubman Centers, Inc., and Belco Oil and Gas, as well as a member of the Advisory Boards of Chase Bank, Chemical Bank, Hydro-Quebec, and the International Energy Corporation.

something that seems actually incredible and is incredible, my objective is by the end of the presentation to persuade you that this almost most incredible thing is in fact real and indeed is a present danger. The danger that must be included in the spectrum of threats by any defence and security establishment that is serious about counter terrorism. Before turning to this topic, though, let me say just a couple of comments in introduction. First, let me commend the Centre of Excellence Defence Against Terrorism for the excellent work that you have been doing, and the command and leadership of the Turkish Armed Forces and the government for their initiative in establishing such a centre. I have been familiar with the work of the centre from a colleague, Dr. Mustafa Kibaroğlu, who is at Bilkent University but who spent a year at the Belfer Center that I am the Director of at Harvard. Looking through the themes of the centre's work last night, I found a huge number of lines that I agree with or applaud.

So just in the material that was provided for us, terrorism is chaos, absolutely. Terrorism is not a new phenomenon, terrorism is all this history, but terrorism continues to have a changing face. And in this proposition, which will be central to my presentation, the *sine qua non* - I am quoting down from the material of the Centre of Excellence Defence Against Terrorism is to establish a conversant and cooperative mechanism at the global level. So I am pleased and applaud the work of the Centre, and especially the work that has taken account, recently, of weapons of mass destruction terrorism and other high-end threads, which will be what I am talking about today.

I was at the dinner last week in Washington in which Secretary of Defence Robert Gates was being honoured and he was being introduced by a long-time colleague of mine, James Schlesinger, another former Secretary of Defence and at the table we were teasing about a comment of another of our colleagues who for many years wrote the US Defence's Posture Statement which is the annual report issued by the Secretariat of Defence. This colleague, William Kaufman, was asked about how different it was writing the annual report for Secretary Schlesinger when he was Secretary of Defence as compared to his predecessor Harold Brown, who had been Secretary of Defence just before him. Bill said: "That's a good question. Jim Schlesinger is actually a big picture man. He focuses on the forest. So in the Defence Posture Report I had to think about the forest, whereas with Harold Brown, who is a nuclear physicist, he actually is a tree man, he focuses on the trees, this tree then that tree and that tree." But he said: "But you know President Jimmy Carter, he is a leaf man. He likes the leaves."

So what I am going to do in the presentation today is, first start off with a little bit about the forest, then very quickly turn my slides which focus on one central tall tree namely Nuclear Terrorism. But first a few words about the forest.

As my predecessor said in the aftermath of the Cold War, one of the biggest challenges for us is a community, and an international security community is the conceptual challenge. And my candidate for one of the new items in the conceptual geography of security in the 20th century, my candidate is the paradigm shift that comes in recognizing that the function of armed forces is no longer only to secure its population against the armed forces attacks of other countries. For the last 2000 years the principle task of the armed forces of a country has been to defend the population against the armed forces of other countries, not the only task but the principle task. But I take 9/11 to be the introduction to the 21st century that requires a paradigm shift that will expand this set of challenges. On 9/11, the attack on the World Trade Centre towers and the Pentagon by a group of 19 individuals who were part of a non-state killed twice as many Americans as the Japanese did in the attack on Pearl Harbour that initiated the entrance of the US into World War II. Think about it! A non-state actor killed at a level that was previously the preserve of states and organized violence that states are capable of. Today and for the foreseeable future, technology has super-empowered individuals and small groups giving them the capacity to kill at a level that was previously only possible and could only be done by organized states. So when one thinks about the challenges of a defence community or an intelligence community or special services, we now have to include in our spectrum of threats and even high-end treats, the possibility that our populations could suffer casualties at a level that were previously inconceivable, to have been perpetrated by anything other than the state, but that was actually conducted by a small group of individuals, individuals who might be global citizens, or who might even be our own citizens. So on the spectrum of threats, of terrorism, they are at a high end. There is what Eisenhower referred to as mega terrorism, that is terrorist acts that can kill thousands and tens of thousands of people in a single blow.

And today what I am going to focus on is actually the first hint of that spectrum: nuclear terrorism, which is the only form of terrorism that could kill hundreds of thousand of people. Hundreds of thousands of people in a single event!

So let me turn now from comments about the forest to the specific issue of the trees, which are the subject of this PowerPoint slide presentation. President Obama has said that nuclear terrorism is the single most important national security threat that the US faces today. Nuclear weapons are in the hands of terrorists. This is precisely the same view that George Bush, his predecessor had. When the UN was preparing for its 60th anniversary celebration it invited a group of a dozen wise men and women from around the world and asked them to think about threats to international security in the next quarter century. They identified 6 major threats of which they gave quite a place to nuclear danger; and about nuclear danger they said - and this is the bottom-line - “we are approaching a point at which the erosion of the non-proliferation regime could become irreversible and result in a cascade of proliferation.” Mohamed El Baradei who along with the International Atomic Energy Agency (IAEA) won the Nobel Peace Prize in 2005 argues similarly: “nuclear terrorism is the most serious danger the World is facing today.” Not just for the US, the World!

Kofi Annan, again a former Secretary General of the United Nations, notes that: “A nuclear terrorist attack can occur anywhere, in London or Delhi or New York, it would cause not only wide-spread death and destruction at that one target city, but it would stagger the world economy and thrust tens of millions of people into property, creating a second death toll throughout the developing world.”

What if? Those of you who were old “Cold Warriors”, who include many in this room, will be familiar with target maps. This is a map of New York City and it imagines that a bomb that was thought to be in New York City a month after 9/11 was exploded in Times Square. I tell the story of this episode in my book "Nuclear Terrorism" where an agent called “Dragonfire” was reporting just a month after the 9/11 attacks on the World Trade Centre that Al-Qaeda had acquired a small nuclear bomb out of the former Soviet Arsenal and had that bomb now in New York City perhaps about to explode. This was an occasion when George Tenet, at the time the director of CIA, came to see President Bush with warnings for the President’s daily intelligence briefings and informed him that this agent who had generally been a reliable source had produced this report. There were then a few moments to catch breath and interrogatory that winds up thing a like this. Did former Soviet arsenal include weapons of the description that Dragonfire had given, and guess? Were all these weapons adequately accounted for? Answer: No! Could Al-Qaeda have acquired one of these weapons and brought it to New York City and be about to explode it, and the US not otherwise know anything about it? Answer: Yes! So on the basis of this interrogatory there was the bottom line conclusion that there was no basis for dismissing Dragonfire’s report that there was a live nuclear bomb in New York City about to be exploded. This was the occasion when President Bush ordered Vice President Cheney to leave Washington, because the fear was there might also be a bomb in Washington. And if that bomb should explode in Washington, the US has a plan back from the old Cold War days that I worked on under the Reagan administration for continuity of government, in which there is an alternative government. Where Cheney together with a couple of thousand people from different agencies of the US government would be the government if the first government were destroyed in the decapitation attack.

Nuclear test teams, nuclear experts from the labs were sent to New York City, they looked for signs of radioactivity. The bottom line of this story turns out to be the good news that this was a false alarm. But the message for us is that on the basis of science, technology, logic, there were no grounds to dismiss Dragonfire's report that there was now a live nuclear bomb in New York City. If this bomb had been put into the back of a SUV, a small bomb that was assumed to have about ten kilotons explosive power, which is slightly smaller than the Hiroshima bomb, then drive the SUV to Times Square and blown up on a work day. The result would be half million people killed in the first few minutes, and another half million could die in the week or so after. So the red zone here you see going around Times Square is about a third of a mile, all of that disappears instantaneously. In this vast release of energy that accompanies the explosion of a nuclear bomb, vaporizes in a blast heat of about 540,000 degrees Fahrenheit, and everything up to a mile, which is the blue line, all the bridges, the UN Building, the tunnels, look like Oklahoma City after a home grown American terrorist bombed a federal office building there back in 1995.

If that seems too far away, here is Dragonfire's bomb in Ankara. You can look at the locations. So as President Obama said in September, just one nuclear bomb, just one nuclear bomb exploded in Moscow, New York, Tokyo, Beijing, Paris, London or Ankara could kill hundreds of thousands of people in a single event. It will not only destabilize our security and our economy, it would change our very way of life.

In the book *Nuclear Terrorism* that was referred to, I have two parts: part one and part two. Part one says inevitable, part two says preventable. The juxtaposition of the two is somewhat paradoxical and requires explanation. So part one of the book argues that on the current track, on the current trajectory nuclear terrorism is inevitable. Proposition two says and part two of the book argues nuclear terrorism is preventable; indeed the subtitle of the book Nuclear Terrorism here is called the "Ultimate Preventable Catastrophe". That is the most important proposition. Nuclear terrorism is preventable by a feasible, affordable agenda of actions, some of which we are not taking, some of which we are not taking fast enough.

So proposition one: inevitable. If the US government and the Turkish government, and the Russian government, and the Pakistani government, and every other government, and the UN, and the IAEA, all the other actors just keep doing what they are doing today, a nuclear terrorist attack in a major city, somewhere in the world is more likely than not in the decade ahead. I wrote that in 2004, that means that in my view, my own best judgment, by the end of 2014 there still remains a better than even chance that is 51%, that is, on the current trajectory terrorist successfully explode a nuclear weapon somewhere in the world now in the next five years.

Interestingly for some of you maybe, there was a commission established by the US Congress as a successor to the 9/11 Commission, called the Commission on Preventing WMD, Terrorism and Proliferation. And it was co-chaired by two former senators, a democrat, Bob Graham from Florida, and a Republican, Jim Talent from Missouri. That Commission issued its report in December 2009 and in its report it says “In the view of this commission, Republicans and Democrats who were looking at the issue and giving their best judgment, they believe that on the current trajectory by the end of 2014 it is more likely than not that a nuclear or biological terrorist attack occurs somewhere in the world.” That does not mean it is correct, but that is a judgment. Warren Buffett, the world’s most successful investor, he is also extremely smart in thinking about risks, because he is in the insurance and the reinsurance business. This is his view; he says, he believes nuclear terrorism is inevitable. I do not see any way it will not happen he says. And then he gives us this interesting mathematical identity just to help those of us who are not accustomed to thinking about the way in which probabilities mount up. He says “If the chance of a nuclear weapon being used in a given year is 10% - he is not saying it is 10%, but if that were how likely it was - and that same probability persists for 50 years, the probability of it happening at least once during those 50 years is 99.5 %." So 10% probability for a year roll that over 50 years and it becomes almost one hundred.

Another way to think about this issue, which I know is incredible, especially to many European audiences, is to ask the views of the individuals who shouldered responsibility for trying to think about this issue, and who themselves take responsibility for dealing with it. Robert Gates, our only Secretary of Defence who served both a Republican and a Democratic President repeatedly says, that he wakes up at 3 o'clock in the morning and thinks 'Oh, my God! Things could be worse'. What is he worrying about? It is the thought of a terrorist with weapons of mass destruction, especially nuclear. Watson who was the American Intelligence analyst who spend the most time working on the nuclear question, argues that the 21st century is going to be defined by the desire and then the ability of non-states to developed crude nuclear weapons, which remains Al-Qaeda’s preoccupation. Former Russian Prime Minister and former Head of Intelligence, Mikhail Primakov, notes that “International terrorists have been especially interested in getting their hands on nuclear weapons in the black markets for nuclear materials technology and expertise."

The current Foreign Secretary of India, Ms. Rao, says "The challenge of nuclear terrorism is a serious nuclear security issue we address. We have been affected by clandestine nuclear proliferation in our neighbourhood and we are naturally concerned about the possibility of nuclear terrorism.”

Secretary Clinton: “The biggest nightmare, all of us have, is that one of these terrorists will get their hands on weapons mass destruction.” Jim Jones, a former general, now National Security Advisor, his biggest nightmare scenario is acquisition by terrorists of a nuclear weapon, it would be a game-changer.

How would we think about the likelihood of an unprecedented catastrophic event? I looked at the various methodologies for doing this. There is no scientifically-based methodology for estimating, but there are various algorithms and approaches for presentational purposes. I settled on what is basically the journalist's checklist who, what, where, when, how.

Who could be planning a nuclear terrorist attack today? What nuclear weapon would they use? Where could terrorist acquire a bomb? When could terrorists launch the first attack? How could terrorists get a nuclear weapon to its target? Who? Osama Bin Laden and Al-Qaeda is the top of my list. But in the book, I give you a list of a dozen other potential perpetrators. Osama Bin Laden has set out the agenda for his group, to prepare as many forces as possible to terrorize the enemies of God. Abu Ghaith, his spokesman said: “We have the right to kill 4 million Americans.” In 2003 two years after the 9/11 attack, Osama got a fatwa from a radical sheik justifying the killing of 10 million Americans with a nuclear or biological weapon. As the 9/11 Commission report says: "Al-Qaeda is trying to acquire or make nuclear weapons for at least a decade and continues to pursue its strategic goal." Bin Laden has been overheard refer to the objective as Hiroshima. Al-Qaeda has clearly not only expressed aspirations but it is engaged in activity that would be aimed at realizing these aspirations. It is trying to recruit nuclear experts. I described in the book two Pakistani nuclear weapon scientists who met with Osama Bin Laden and his deputy al-Zawahiri in Afghanistan to talk about nuclear weapons. The IC Commission, another of this post 9/11 Commissions concluded that Al-Qaeda probably had access to nuclear expertise and facilities, and that there was a real possibility of their developing a crude nuclear device. Fabrication of such a device is within their capabilities if only they could obtain material.

So that is the who, now the what. What bomb could a terrorist use? A ready-made weapon from the arsenal of one the nuclear weapon states, or what is called an IED, and improvised nuclear device, constructed from highly enriched uranium or plutonium stolen from a state stockpile. This is the analogue of the IEDs, the improvised explosive devices, which have been used successfully in Iraq and now in Afghanistan. As Johnny Foster, a former director of one of the US weapons labs and a famous bomb designer, now back more than one quarter century ago, 25 years ago, said: “If the essential nuclear materials are at hand, it is possible to make an atomic bomb using information that is available in the open literature.” Another former lab director Harold Agnew has said: “If you believe that it is easy to make an improvised nuclear weapon, you are wrong. But if you believe it is impossible for a terrorist group to make an improvised nuclear bomb, you are dead."

Where could a nuclear weapon come from? Well, I would still say the most likely source of weapon material is Russia or the former Soviet Union. Not because Russia would want a weapon or material to be stolen. Indeed, a huge amount of work has been done extremely positively by the Russian government and Russian security services to secure Russian and former Soviet weapons and materials in the period since 1991. But because there are so many weapons and so much material I would still say that it is high up on a list.

North Korea is also a possible source of weapons or a weapon for a terrorist group. Today having ten bombs worth of plutonium and having conducted two tests. In my course at Harvard I asked the students "Could Kim Jong-il, the leader of North Korea, imagine that he could sell a nuclear bomb to Osama Bin Laden and get away with it?" For many this seems incredible. And then I asked them "Could Kim Jong-il imagine that he could still be doing something thousands of times larger than a nuclear bomb, selling a plutonium-producing reactor to Syria? Which in fact he did, and which would have been operating today if it had not been destroyed in an air attack by the Israelis.

Pakistan is the world's most dangerous country. I am extremely heartened by the efforts that the Pakistani government has made in recent days, and especially the Pakistani army. But I would still say Pakistan remains the world's most recent country having tripled its arsenal of nuclear bombs and materials since 2001, as the state is challenged internally by a set of ongoing challenges that threatens to overwhelm the forces of order.

And in addition, there are more than a 100 research reactors around the world, 40 in developing and traditional countries that hold either highly rich in uranium or plutonium. Here a piece of very good news. The last element of highly enriched uranium in Turkey that has one of the research reactors was repatriated in December 2009.

When could terrorist conduct this nuclear attack? If Dragon had been correct, a month after 9/11 a nuclear bomb would have exploded in New York City. If terrorists acquire a hundred kilograms of highly enriched uranium, the task of making it into a nuclear bomb will take less than a year.

And how would terrorist get the weapon to the target? The same way illegal items come into our countries every day. I don't need to lecture to folks here about the challenges Turkey has with its huge borders and very difficult neighbours including in particular folks in the Caucasus. The large numbers of ships that pass through the Bosporus include some who carry cargoes of uncertain character. I would say terrorists who have got a bomb or materials to make a bomb, and who are going west; if they are coming out of the territories to Turkey's east, Turkish borders and even Turkish territory are among the most attractive transit routes. And it is Robert Oppenheimer who was the head of the famous Manhattan Project, that made the first nuclear bomb, who said, if you try to ask how you find the weapon or the material that was being smuggled, you basically have got to go into each cargo container, into each unit to get a good read of what might be in it.

So who, what, where, when, how? I do this calculation in the days when I am pessimistic. I said the current trajectory, God forbid; we would live to see a successful nuclear terrorist explosion somewhere in the world. So that's the bad news.

Now the good news! The good news is that this is a preventable catastrophe, that the only terrorist attack, that could kill thousands of people in a single blow, tens of thousands, hundreds of thousands in a single blow, is preventable by a feasible, affordable agenda of access. Warren Buffett again comes to the rescue to remind us that if our actions that we take to reduce a probability that has been 10% a year to just 1% a year, and if we run that over 50 years, there is a 60% chance this never happens. So let it be clear. Our actions affect the likelihood of this event, and if we took the actions that we could take, and reduce the chance to 1% a year, then it would be 60% that over 50 years this did not happen. And there is nothing magic about 1%. How about 0,10 %. Then it becomes unlikely to happen in several hundred years. So our focus should be on the actions we could take to shrink the likelihood of this to nearly zero. How to prevent it? Obviously this is a challenge that requires multi-way defence. So there is not just one thing to do. Obviously it requires a 360-degree approach. But fortunately there is a strategic environment now that allows us, if we were able to focus on the supply side of this issue in a way that would allow us to be successful in preventing nuclear terrorism. And this good fortune occurs because of a happy syllogism from physics. So the syllogism from physics is no fissile material, no mushroom cloud, and no nuclear terrorism.

Let me explain. Fissile material comes in only two brands: highly enriched uranium or plutonium, neither current in nature. So you cannot just find them and dig them up. Each requires huge manufacturing efforts, a multi-billion dollar dedicated effort to make highly enriched uranium or plutonium. Therefore, this will not be done successfully by terrorist running around in villages or caves. So only states make highly enriched uranium and plutonium. So no fissile material, no possibility of this release of energy that makes a mushroom cloud and therefore no nuclear terrorists. So as a consequence, all that we have to do - it is a big goal, but still it is clear - all that we have to do is prevent terrorists from getting fissile material either in the form of a bomb or from which they can make a bomb. So by denying them the means for their deadly aspirations we can actually defeat nuclear terrorism. Now, how to do that?

I try to organize a strategy for that under a doctrine of three NO's:

(1) No loose nukes;

(2) No new nascent nukes;

(3) No new nuclear weapon states.

Let me say a word about each. "No loose nukes" requires securing all nuclear weapons and all weapon-usable material as fast as possible. In America when I made this presentation I asked how much gold does the US lose from Fort Knocks, which is the place where the US keeps its gold reserves. And the answer is: "not one ounce."

In 2006 I was invited to make a presentation on nuclear terrorism in Russia at the Kremlin. And I made basically a presentation like this, and I asked with all the chaos, all the confusion, and even the corruption that accompanied the collapse of the Soviet Union, "How many of the treasures of Russia that are kept in the Kremlin armoury, the icons and crowns and other treasures, how many are missing?' The answer: Zero! So human beings know how to lock up things that we do not want people to steal. The challenge is to lock up all nuclear weapons and all nuclear materials to this gold standard.

The second no is "no nascent nukes". Nascent nuke, I apologize, is a neologism for new national enrichment of uranium or production of plutonium. One should not think of a facility that produces highly enriched uranium as a producer of fuel for a reactor which some would like to try to make us believe. In fact highly enriched uranium or plutonium should be thought of as nascent nuclear weapons, that is nuclear weapons that are just about to hatch. In the second no, we should have "No new national enrichment of uranium or reprocessing of plutonium. It is urgent to challenge this "no" in Iran. In 2004 Iran had zero centrifuges and enriched zero new uranium. Today, right now, today Iran is running 4,000 centrifuges producing a new and additional 8 pounds of low enriched uranium every day and it has accumulated a stockpile of over 4,000 pounds of low enriched uranium which, when further enriched, would become the stuff for two nuclear bombs.

The third no is "No new nuclear weapon states", and proposes to draw a line under the current 8.5 nuclear powers and say unambiguously stop, no more. Let me say it clearly, the idea is not to maintain the current nuclear state for ever, but rather to stop the bleeding before we address the question: What should be done about the arsenals that are currently in existence? The huge challenge to this proposition is North Korea which again in the periods since 2001, 2002, 2003 indeed has gone from having at most two bombs worth of plutonium to the situation where it has 10 bombs worth of plutonium and has conducted two tests. And the Yongbyon reactor it's now being refurbished to be turned on again. But it is harvesting the spent fuel rods at that reactor for its 11th bomb.

Each one of these nos produces then the need for a strategy and an operational plan of action that becomes thick. But let me just give you a couple of the bullet points and then I will stop for short.

No loose nukes as global gold standard, the principle of assured nuclear security that would be transparent enough to allow leaders of one country to assure their own citizens, the terrorist will not get a nuclear weapon from another country. Signing up to this principle of assured nuclear security, and a global clean-out of all fissile material that cannot be secured to a gold standard. So this is: no loose nukes, no new nascent nukes. It says orchestration of the whole array of carrots and sticks to persuade, to postpone enrichment activity. I would say currently the best that could be done, would be to stop where it is now. And I think the proposal made by the IAEA to trade the current stock piles of low and rich uranium for the fuel rod that are needed for a research reactor, that make medical isotopes, is a very sensible proposal. And the international community should be pressing Iran to accept it. Turkey played a very important role in this, in offering to be the last resort for the transfer. A multi-laterally guaranteed fuel bank. This is another IAEA initiative that was actually just started by Warren Buffett who provided just from his private fortune 50 million dollars to the IAEA to create a multi-lateral fuel bank managed by the IAEA as a supplier of fuel for peaceful civilian nuclear reactors of last resort. And then in five or ten years a moratorium on further enrichment to try to revitalize the non-proliferation regime.

The third no, “No new nuclear weapon states”, is concentrating all its efforts on North Korea. At this stage the only hope is that China should be motivated to persuade North Korea to freeze nuclear production and over time to work on verifiable dismantlement. I am also a strong proponent of a new principle of deterrent which I think will get a lot of discussion. I hope, I expect this will be in the US Nuclear Posture Review, which is just forthcoming, the principle of nuclear accountability according to which a state would be held accountable for the nuclear weapons and materials it makes no matter how those nuclear weapons or materials might come to be the stuff of a bomb that explodes in another state.

As to the current administration, I am not here as a spokesman for the Obama Administration or the US Government, I have many friends and colleagues in this administration, I advised or offered my views to as I did to the previous administration. But I would say about President Obama, we have a president who gets it, in the sense, that this is a question and issue he has internalized. When he is given a chance to talk about it, he talks about it with some passion. In his first international speech, which was in Prague in April 2009, he gave a speech about nuclear weapons and nuclear danger in which he addressed, for instance, the issue of reducing the role of nuclear weapons in the US national security strategy. This will be evident in the Nuclear Posture Review.

Securing all nuclear weapons and materials to this gold standard in four years, this will be the focus of the nuclear security summit which will be held in Washington with 42 heads of state just next month in the middle of April, negotiating new arms control agreements, in particular to follow Start, which US and Russia have been fooling around with, but will come to a conclusion here very shortly ratifying the Comprehensive Nuclear Test Ban Treaty (CTBT), outlying future nuclear weapons tests and stopping all production of fissile material. And then a strong IAEA, in particular with more authority and more resources.

So this nuclear terrorism, as was mentioned, offers my best attempt to make the case that first, this is a real present danger, and secondly that it is a preventable catastrophe. It has been reasonably well reviewed. And I would say, it is not necessarily correct, but it is closest to the proposition, that this is a threat, an ultimate threat that we face as part of the new security environment. But that is a preventable threat, preventable by course of action that we could take if we get ourselves together, but then we can only take if we do it in an international, cooperative fashion. There is no way this is a numeric agenda; no way can an American agenda of this topic succeed by itself. I would say lots have been done, particularly in the Russian-US relationship through Cooperative Threat Reduction (CTR). A lot has been done through the global initiative to prevent nuclear terrorism and Proliferation Security Initiative (PSI). A lot has been done by individual states. Lot of work has been done. That's the good news.

The bad news is that we face powerful adverse trend lines that continue eroding the regimes and continue increasing the likelihood that somehow, some day, somewhere a terrorist groups, perhaps Al-Qaeda, perhaps even some other group, will get a nuclear weapon and will explode it to destroy one of our cities. And that will change our whole security environment that will change our whole notion of economic globalization that will change the whole way we think about the world.

So to conclude, I would say, this is the high end of a spectrum of threats. It is not going to go away. It is an issue for the foreseeable future. It is not the only thing at the high end. There is another topic of bio, that's another big and complicated subject, and there are other things that are at the high end. This is at the high end, this I think is real. This I think is preventable.

So, thank you for the opportunity to present.

General Stéphane ABRIAL (FRANCE)*

Supreme Allied Commander Transformation (SACT), NATO

Thank you very much for your kind words, thank you also for your activities as Head of the Centre of Excellence for Defence Against Terrorism, and thank you for organizing this important symposium here in Ankara, bringing together so many of the most eminent names in this field. Thank you also very much to General Başbuğ for hosting this conference and honouring it with your presence for the in-depth and thought-provoking insights he shared with us earlier, and on a more personal note to this first official visit I make to Turkey as Supreme Allied Commander Transformation: Turkey is an essential ally as well as a key contributor notably in Afghanistan and a great support for allied command transformation. And I have been very much looking forward to this visit and our coming discussions.

Excellencies,

Generals, Admirals,

Distinguished Guests,

Ladies and Gentlemen,

* Gen. Stéphane Abrial received appointment by the North Atlantic Council as Supreme Allied Commander Transformation on 29 July 2009. He is the first European to be appointed permanently as head of a NATO strategic command. Born in 1954 in the South-Western French department of Gers, he began his military service in 1973. After an exchange program in US Air Force Academy, Gen. Abrial graduated from the French Air Force Academy in 1975. He completed his pilot training in 1976. Gen. Abrial has extensive experience both as a fighter pilot and an operational commander. He has a wide ranging background that includes operations in coalition environments, at the tactical, operational and strategic levels. He served in a unit of the German Luftwaffe from 1981 to 1984 and with a unit of the Greek Air Force in 1988. In 1990 and 1991, he took part in the liberation of Kuwait as commander of the French Air Force's 5th Fighter Wing during Operation Desert Storm. From 1996 to 1999, he served at the NATO International Military Staff in Brussels. He is a graduate of the U.S. Air War College, Montgomery, Alabama, in 1992, and of the French Institute for Advanced Studies in National Defense (IHEDN) in Paris. He acquired broad experience in political-military matters through several appointments to the private offices of the French Prime Minister and President, and went on to serve as head of French air defense and air operations, and finally as Air Force Chief of Staff from 2006 to 2009. He has, among other distinctions, been elevated to the rank of Grand Officer in the French Legion of Honor, and Commander of US Legion of Merit, and was awarded the German Verdienstkreuz der Bunderwehr (silver). Gen. Stéphane Abrial and his wife Michaela have two teen-aged children.

Because of that I am going to adopt a different approach to the subject of terrorism, and to how terror is observed from the perspective of a strategic commander of NATO. Perhaps for the first time NATO mentioned article five that governs the response to any attack on the Alliance. It was very difficult to consider this at the time the Washington Agreement was signed. But when we consider the threats today, the threats are not coming from states, but technological developments have made it possible that highly damaging weapons end up in the hands of some non-state actors. And the latest developments have given them the power to undertake that. But although some terrorist activities are observed in some NATO countries, NATO was not attaching much importance to deterrence. The attacks in New York on the Twin Towers, in Istanbul, in Madrid and London have changed the whole situation.

When we consider the current strategic environment, no NATO country is very likely to be attacked by another country. Non-state actors or entities are the real threat at the moment. Before the Washington Agreement, they were not thinking much about how to equip NATO countries for example with Awacs. But the agreement brought the organization closer together – out of necessity. It was understood that there is a security problem facing the Alliance. The problem was taken up. NATO had to change because of that, and the biggest reason was to be able to combat this new threat. The position of NATO has developed extensively as compared to two decades ago. We have to continue to transform and adapt ourselves, to harmonize our efforts, because the terrorist threat is an entirely new challenge to be confronted.

After 9/11, the Alliance realized that the security of a transatlantic region could depend on the ability to intervene in areas that may be thousands of kilometres away. This realization has been a main driver in our organization’s development of an expeditionary capability in what was at first called “Out of Area Operations," a phrase that has now interestingly lost much of its significance. An important milestone in this evolution was the establishment of a NATO response force ready to be deployed at short notice within or beyond the Alliance’s traditional region of interest. This has marked a profound cultural shift reinforced by the reality of today's operations. Our most pressing current engagement in Afghanistan is as much about counter terrorism as it is about counter insurgency and nation building. Counter terrorism in this context is a strategic concern, in that NATO's intent is to deny terrorists a safe heaven in which to organize, train, plan and act, including on alliance nations’ territory.

Today the most powerful way of doing so is in capacity building, Helping Afghans themselves develop capable and self-sustaining security forces able to perform these tasks particularly through NATO training mission in Afghanistan. Within this operation, we are also confronted with terrorism at the tactical level, as terrorist techniques are often employed by insurgents. One important aspect of our engagement in Afghanistan has been the fight against improvised explosive devices, IEDs, for which ACT has been specifically tasked to coordinate NATO efforts. IEDs accounted last year for two in every three fatalities suffered by ISAF troops, as well as the death of many Afghan civilians. One may legitimately debate whether all IED attacks against major targets qualified as terrorism, or if some are irregular insurgency tactics. But what is certain is that defence against IEDs is an action of counter insurgency and counter terrorism. We must focus vigorously both on the requirement to train our forces to operate safely and effectively in an IED polluted environment, and – underneath – to neutralize and dismantle the whole of what we call "The IED Network" or "IED System", from the financiers to the planners to the hardware itself.

This calls for a range of different actions but they are highly transferable from defence against terrorism whether intelligence management or in countering explosive devices. Such supporting networks and the devices employed could easily find their way into our own countries, in one form or another. And although our collective experience in countering them in operations has already been put to good use in allied nations homeland defence. Our shield is far from unbreakable, though. For all these reasons, the fight against IEDs has driven us to collaborate more and more with specialists from the civilian law enforcement side of counter terrorism, a group of professionals who were well represented at a conference organized by ACT and hosted by Hungary in Budapest last month.

NATO's operation in Afghanistan is the Alliance's most visible and prominent action in defence against terrorism, but it is clearly not its only contribution. Our efforts, our multi-faceted efforts span the whole spectrum from counter terrorism to anti-terrorism, consequence management, stabilization and reconstruction. We take a lead role in some cases and a supporting role in all others. Our involvement begins at home notably in the green but critical area of consequence management. It is our job as military to prepare for the worst and particularly for the gravest of foreseeable threats upon which Prof. Allison has written and spoken to this audience so vividly. Weapons of mass destruction being used by terrorists would have disastrous effects. NATO is working on ways that military capabilities such as civil engineering, medical or decontamination teams could be mobilized to contribute in mitigating the destructive or secondary effects of such attacks. Our NATO Euro-Atlantic Disaster Response Coordination Centre and the Alliance's Senior Civil Emergency Planning Committee are well prepared to be the focal points of such a collective response. We are determined, however, to keep such a disaster from happening in the first place. One of our most important fields of activity is preventing the exploitation by terrorists and other disaffected non-state actors of the environments C-R space and cyber space often designated as the global commands. We need both to guarantee our freedom of movement in these domains which are vital to our strategic flows, and to deny them to those who wish to do us harm. In dealing with the global commands, it is fundamental to respond multi-nationally. By the very nature, these pan-national borders in purely-national responses may create even greater vulnerabilities that our adversaries would readily exploit.

Nations must work together to create a global environment that is unattractive to terrorists and other criminal elements, but secure for legitimate travel and trade. NATO plays an active role in SP security. It is also alert to the importance of countering cyber attacks; particularly attacks aimed at causing loss of life. Our Cyber Defence Centre of Excellence in Estonia serves a vital purpose in this regard.

However, the part of a global command in which NATO has been the most widely involved is the maritime environment. You will recall that hostile acts have been successfully delivered from the sea against our forces. Remember the USS Cole in 2000 and the attack against the French oil tanker Limburg in 2002 with the intention of disrupting strategic flows. An additional complication is that this environment has favoured smuggling of people, weapons and illegal materials. Denying terrorist free access to maritime spaces is a principle motivation behind NATO's operation Active Endeavour. It was launched in the aftermath of 9/11 and I would like to mention here that the Turkish navy is a major contributor. This operation has been monitoring shipping through critical choke points with the specific intend of detecting and deterring terrorist activity. It has been significant for its immediate effect. Active Endeavour has checked over 100,000 merchant vessels and routinely boarded suspect ships. But its existence is also important for the awareness of the environment and traffic patterns they give to the nations, as well as putting our forces' surveillance, command and control skills to a real life test.

Indeed NATO’s technical expertise is developing on a number of fronts informed by the experience from these operations. ACTs on NATO’s Underwater Research Centre in La Spezia Italy has a leading role in improving the Alliance’s capabilities for maritime force protection in ports and harbours, including through the investigation and trial of several new technologies. The centre is working in close coordination for example with the Confined and Shallow Water Centre of Excellence in Kiel, Germany, and with many others who will take part in the international Waterside Security Conference to be held in La Spezia next November. The Centre is also working on mine counter measures to improve NATO nation’s capabilities to protect ships conducting expeditionary operations.

Another related field we at ECT are working on is improving the ability to conduct investigations of vessels by developing a comprehensive capability for the detection and identification of chemical, biological, radiological and nuclear materials smuggled in containers, or otherwise shielded. The maritime environment would be the first in which we will experiment this capability. It is indeed the area we have identified as carrying the highest risk for elicit trafficking of such materials. We then hope to transfer it to the land and environments. Naturally, NATO's engagement in finding technological responses to the terrorist threats goes beyond these examples. The Conference of National Armament Directors has made defence against terrorism a priority with a wide-ranging program of work focusing on issues extending from protection of large-body aircrafts from Stinger-like non-portable air defence systems to counter IED or consequence management.

However, technological solutions take second place to an even more crucial issue, that of cooperation, networking and information sharing. And let me draw again from the experience of operation Active Endeavour which has developed through the years in a very encouraging manner in a way that can be used as a blueprint for broader, permanent cooperation. The international support for this operation has indeed been very encouraging. On the military side, we have seen a number of non-NATO countries even contribute, support or express interest in taking part in it. Ukraine has participated several times, as has Russia. Defence against terrorism is a powerful venue for military-to-military cooperation and more generally for trust-building around common security concerns. Active Endeavour has also forced new levels of interaction with national authorities, particularly civilian both within the Alliance and in partner nations such as members of the Mediterranean Dialogue. The natural evolution of this operation is its current transition from platform-based to network-based; relying above all on the network of collaboration it has developed through the years.

Let me insist on the critical importance of information sharing in the defence against terrorism. Classified and unclassified information is the lifeblood of our efforts. And one of the key fields in which the military can uniquely contribute thanks to intelligence surveillance and reconnaissance capabilities. But even more essential than collecting intelligence is ensuring that it gets into the right hands and in time. This means doing much better in sharing with other agencies or other NATO organizations and indeed with partners, international organizations, and even non-governmental organizations. We are making progress. NATO for example, is conducting a review of its classification system and is encouraging nations to ease these types of transfers. Some measures are technical, such as improving interoperability of ISI systems. But once again the key is culture.

Building trust with the best possible intelligence means sharing information at the lowest possible level, without having been sanitized to the point of rendering it useless and fast enough for it to be actionable by the end user. The issue of intelligence sharing is one of my main concerns in our fight against IEDs in Afghanistan. I am encouraged by the fact that ISAF will soon be implementing the Afghan mission network, which will significantly improve our ability to share and fuse information between all nations with appropriate actors contributing to our effort. But some obstacles remain. The development of a biometric capability is being hindered by technical procedure and legal limitations in information sharing. Such a capability would clearly have defeated the systems and networks behind the IED devices.

I have called the Ministry of Defence in all member nations to conduct, as a priority, a review of the obstacles to sharing such critical information. Learning lessons from our engagements and experiences is a related field in which I am determined to see ECT make a positive contribution. Our Joint Analysis and Lessons-Learnt Centre in Lisbon Portugal not only produce its own quality results, but it also helps share national experience more widely among the nations. Nowhere is this more necessary than in defence against terrorism.

In these issues of cooperation and information sharing, I would especially like to salute the great role played by our hosts, the Defence against Terrorism Centre of Excellence in expanding our networking with partners. The fact that in 2009 almost half of the participants in this COE’s courses were from non-NATO nations is an eloquent illustration of its attention to outreach. Responding to terrorism multi-nationally and particularly within NATO is highly appropriate given the nature of a threat, we do not know and which does not respect national borders. But neither do our adversaries respect other boundaries, such as the distinction between civilian and military realms. Note that we acknowledged limits separating terrorism, common criminality, irregular or conventional warfare. Indeed a key insight of a multiple faceted project, the forward looking work ACT published a year ago, was to consider much of modern terrorism as a component of a wider hybrid threat spanning diverse tactics or moving from one to the other as opportunities present themselves. NATO understands that our adversaries in Afghanistan and elsewhere engage in a series of disruptive activities some of which call for a specifically military response, others for a law enforcement approach, and many for a combination of the two; creating the ability for us to better coordinate and train with other security providers.

In finding the right response to this challenge, we too must therefore think more comprehensively, and understand that creating a global environment, inhospitable to such violence, calls for development and security to proceed hand in hand. I am therefore committed to a more efficient and integrated comprehensive approach to crisis management and beyond, based on three principles.

First that we, military bear a crucial responsibility in helping make this comprehensive approach operational. Both upstream of operations and inter-field we must meet other stakeholders more than half way. Military and civilians, players from other agencies, international organizations as well as from non-governmental organizations. Ultimately we should seek a flexible framework that addresses the conflicts and judgments of these actors while respecting their various mandates and cultures.

Secondly succeeding in this depends not only on technical arrangements but on a mindset that must permeate our forces and our headquarters. We must systematically take into account the diversity of players. And finally, our first contribution to a comprehensive approach is to first to do our core job, to provide security. And then to be a catalyst and enable others to do this. I believe this must be the driving force for continued transformation as an Alliance. It will make it stronger in facing the whole range of hybrid threats notably in its terrorist manifestations.

My closing assessment is that defence against terrorism has truly become a central concern of our Alliance today. While it does not in anyway supplant our more traditional duties in collective defence, it impacts widely on our way of doing things. It makes us emphasize civil-military interaction even more and enhances the importance of our partnerships. I have no doubt that the new strategic concept will reflect this concern prominently, and re-energize our collective approach from networking to focus technological research or information sharing. The seeds for what needs to be done are already planted. I am confident that we will soon see progress on many fronts thanks in non-small measure to the work of institutions such as the Centre of Excellence Defence Against Terrorism.

Following in the steps of a great and visionary Turkish Leader, Mustafa Kemal Atatürk, we are all dedicated to “Peace at Home, Peace in the World”. Our populations rightly want to see NATO visibly make them safer, and expect us to deliver in this field, and we will.

Thank you!

f. Dr. Yonah ALEXANDER
Mr. Ahmer Bilal SOOFI
Supreme Court of Pakistan
Speaker
PEACE AT HOME, PEACE IN THE WORLD
YURTTA SULH, CIHANDA SULH

FIRST SESSION

THE ROLE OF INTERNATIONAL LAW AND ORGANISATIONS IN COUNTERING TERRORISM

Chairman:

Prof. Dr. Yonah ALEXANDER
Potomac Institute for Policy Studies

Speakers:

Dr. Andrea ELLNER
King's College London

Mr. Ahmer Bilal SOOFI
Supreme Court of Pakistan

THIS PAGE IS INTENTIONALLY LEFT BLANK

Dr. Andrea ELLNER (UK)*

"A Perspective From Europe"

Good afternoon ladies and gentlemen!

Thank you very much for your kind introduction and thanks also to COE.DAT for inviting me to come for a second time, this time to a much larger event, and to speak to this distinguished audience.

The reason is that I am focusing very much on my European perspectives, and on the question of "What does the EU do?" In terms of counterterrorism, how does the EU understand terrorism? The phenomenon of terrorism: how does it intend to tackle it? The reason why the EU is a very interesting case study is that the EU has successfully managed to turn itself into a security community which cooperates and is integrated to such a degree that it is - currently at least - unthinkable that European Union countries would go to war with each other.

Yet as you will see in a rather high-speed presentation, there are still huge problems in coordinating counterterrorism and strategies and approaches, which should give us an indication of how much more difficult it is likely to be further outside the EU. How does the EU see counterterrorism? From the start, it has always defined terrorism as a crime rather than an act of war. It has a strong focus on the international, not the internal dimension; and I will explain why that is the

* Dr. Ellner joined the Department as a Lecturer in Defence Studies in September 2007. Prior to this she lectured for nearly 10 years on International Security Studies and related subjects at the University of Reading, where she also led the Graduate Institute of Political and International Studies for three years. In 2006/7 she served on the Committee of the University Association of Contemporary European Studies (UACES). In 2005 she was a visiting lecturer at the Ecole des Hautes Etudes en Sciences Sociales, Paris. She is also Programme Leader European Security and Transatlantic Relations, Centre for Defence and International Security Studies (CDiSS), and Editor-in-Chief of the journal European Security. Dr. Ellner received her MA in History from the Ludwig-Maximilians-University, Munich, and her Ph.D. in Political Science on British Naval Policy, 1970-1990, from the Free University of Berlin. Dr. Ellner's some selected publications and conference papers are: "Developments in CFSP", (CFSP Forum, 2007), "Regional Security in a Global Context", presented at the Conference on "Security in a Changing World: Discourses, Changes, Realities," (Yıldız Technical University, İstanbul-2007), "Curbing Nuclear Proliferation: An Impossible Task?", Presentation at Sandhurst Defence Forum, Royal Military Academy-2005), "European Perspectives on Security - Lessons of the Conflicts in the Balkans, the Middle East and Africa", (Washington, D.C. -2004).

case. But it recognizes the interdependence of internal and external security in our globalized world, and dealing with terrorism as a truly global phenomenon.

I will briefly talk about the European Security Strategy because the European Counterterrorism Strategy is explicitly linked into the European Security Strategy. We have already talked about this, and you will find that much of what I'm saying links in very well with what we have heard this morning. Many of the concepts we have talked about will appear within the context of the EU approach as well. The EU thinks of itself as a particularly well-suited actor able to implement a so-called comprehensive approach. I will explain in a moment why that is still very difficult. The European Security Strategy was very much a product of the transatlantic crisis of Iraq where the EU was really challenged to define what it did and did not want the US and coalition partners to do." It did not say what it wanted and where it stood. So it defined itself as an actor who was trying to strive for a "more secure Europe in a better world;" this is the title of the strategy. The strategy is broadly rooted in a human security approach. It links internal and external security of course, in the context of globalization, and the dependence on network infrastructures.

And amongst the threats - not the only threats it identifies, but the ones relevant to us here – it identifies the principal ones of WMD proliferation, terrorism, regional conflicts including frozen conflicts (of which there are quite a few in Europe), state failure and organized crime. It imbeds that in an assumption that there is a need to address the - what I call - "Dark Sides of Globalization;" in particular poverty, which can often be linked with state failure. And it tries to achieve these goals primarily by promoting effective multilateralism. It does this because it assumes that its own model of building community, security and stability can actually be exported to the rest of the world. In my paper I go into much more detail on this, and if you are interested, you can read it up there.

Thus the assumption is that the best foundation for security is a world of well-governed states; and in order to bring that about, it seeks to strengthen international order through effective multilateralism, spreading good government, supporting social and political reform as well as economic development, dealing with corruption and abusive power, adherence to democratic principles, establishing the rule of law, and protecting human rights. So the overarching framework has quite normative aspects. It relates to international law. It aims to spread common norms and norms of behavior. It seeks to address the root causes of terrorism, not just the symptoms – in fact I would say it is much harder to address the root causes, which is of course a long-term thing – and it seeks to do all these while promoting security and the protection of civil liberties internally and externally.

It is important to understand that the EU's efforts on counterterrorism that are not directly linked to common foreign and security policy are very much related to the development of internal, almost domestic cooperation on law enforcement and in traditional matters. This started in the 1970s but was all very informal. It began with the Maastricht Treaty which established a single market, and with it the internal borderless area of the EU; there were new challenges arising to combat crime because border controls were suddenly absent. So border controls having moved to the outside, internally it became necessary to start thinking about how to enforce law in order to keep the EU area secure. So it combined the strengthening of external borders with the internal cooperation on law enforcement and in traditional affairs.

Particularly relevant here is the 1995 establishment of the Schengen area, followed in 1998 by the establishment of the European Judicial Network in criminal matters; and during the same year, the Vienna Action Plan on judicial cooperation. With the Maastricht Treaty at the end of the 1990s, the EU established a different area, calling its internal region "the area of freedom, security and justice," and the focus was very much on further strengthening the security of the internal freedom of movement, protecting the area against terrorism, organized crime and fraud (including money laundering). It also promoted cooperation of police, especially Europol, which was established in the late 90s. Another area was judiciary cooperation on civil and criminal matters, both internally as well as with external partners. There were at the time - and there are still - lingering fears that there is something of a fortress Europe emerging; in other words, that Europe sends out the message that internally the EU area is to be kept secure. This means that people who may or may not justly be suspected of actually bringing insecurity into the EU may be kept out; and the external borders are the dividing line. That is an issue of considerable consent of quite a few academics.

Within ten days of the 9/11 attacks, the EU came up with an action plan which built on the already emerging security structures in terms of law enforcement and criminal issues. Apart from of course expressing their solidarity with the US but emphasizing that it could be a huge and grave mistake to equate this kind of terrorism with the Muslim faith, it then proceeded to develop a number of steps with which it would approach its counterterrorism strategy.

One of the EU's most basic assumptions is that counterterrorism is really only effective if based on an in-depth political dialogue with those countries and regions of the world in which terrorism comes into being. Of course, that is also partly internal to the EU. And so it is necessary to seek to build strong and sustainable communities for combating terrorism by integrating all countries into a fair worldwide system of security, prosperity and improved development. More concretely, two main outcomes emerge from the action plan: A definition of terrorism and the European arrest warrant.

Without going into extensive detail, the European Arrest Warrant is essentially based on the idea of citizenship of the Union and it replaces extradition and agreements between pre-existing member states. The key issue is that it allows the application of the law of one member state in another member state under certain circumstances if a serious crime has been committed. It is a contentious issue, but it is also quite a revolutionary area.

Now civil liberty organizations have basically complained quite a lot that there was a lack of adequate legal safeguards for individuals who are being pursued under the EAW. The EU actually has defined terrorism; I'll define it once more. I don't have the time to go into very great detail, and you can read up on that in the paper, but the revolutionary thing about it is that it actually defines acts that, given their natural context, may seriously damage a country or an international organization, and that are committed with the aim of seriously intimidating a population and duly compelling a government or international organization to perform any act. Seriously destabilizing or destroying the fundamental political, constitutional economic or social structures of a country or an international organization is to be defined as terrorism. The important thing is that this definition had to be incorporated into the laws of all the EU member states. In 2005 the EU presented its counterterrorism strategy, which in fact unites many of the initiatives it had already pursued, categorizing them very much in the British way into "prevent, protect, pursue and respond."

A basic assumption concerning the EU's role underlying the strategy is that member states really are primarily responsible for countering terrorism. But the EU could add value by strengthening national capabilities and coordination; for example through sharing knowledge, sharing best practice approaches, and defining what needs to be done for critical infrastructure protection and response mechanism, as well as – and that is an important aspect – victim support: in other words, EU-established networks to assist victim support. And it seeks to foster intelligence gathering; more about that later.

Facilitating European corporation at the EU level, the idea that you can contribute to police and judicial cooperation through coordination. But that's also the next step: developing collective capability through the establishment or with the enhancement of organizations established over internal security issues, such as Europol, Eurojust, and EU Crisis Monitoring and Response Organizations. And of course promoting international partnership! So where did the EU go with all these? Where are we now? Police and judicial cooperation, as well as intelligence gathering which I'll also talk about, has been more effective horizontally than vertically; in other words, among member states. The EU has sometimes been more successful in coordinating cooperation between groups of member states than through a top-down or bottom-up approach. It is now enhancing expertise in various forums within the EU.

The EU has, through CEPOL the European Police College, started to define common standards for training. I looked at their website the other day, and they are also looking at conducting training on IEDs. It has had a counterterrorism coordinator since 2004, however this coordinator has very limited power. It has succeeded in improving information exchange including European-wide warrants which allows countries' national authorities to request evidence including DNA, fingerprints, car registration etc., and to transfer or request that evidence from another member state.

So while horizontal cooperation works reasonably well, cooperation and data collection is very difficult because member states - especially the big ones - are very reluctant to share intelligence. The council maintains blacklists, one for which it receives data from the UN and the other which is put together by Europol. The blacklists are on one hand very good monitoring devices, but at the same time the European Court of Justice has repeatedly ruled that they are arbitrary, because the criteria for inclusion on and removal from the list are not very clear. Intelligence gathering and exchange are very, very difficult areas. I have already said that the biggest states are very reluctant to exchange intelligence.

Certain reorganizations under the Lisbon Treaty may actually make it easier to share intelligence, and at the very least, to enhance information sharing through cooperation of these bodies. The goal is to try to generate the kind of trust that is necessary for intelligence sharing and to begin at a relatively high level. But of course there is always a problem that if you are in a multilateral organization with such large numbers of members, many members will be very reluctant to share intelligence between individual members, all members of the EU and third parties. But it has cooperated strongly with the US.

The question of protection and response, maritime and coastal security is assessed by analysts as having significantly improved, but member states resist the idea that the EU should have a major role in critical infrastructure protection. For this reason, it hasn't gone very far, apart from coming closer to some negotiating on what critical infrastructure is. But they have conducted training exercises for response to terrorist attacks, both conventional and CBRN, amongst the EU members, UN and NATO. The monitoring and information center is one potentially quite useful device because it pools member states' resources. Member states can then request them within 24 hours, but as I said before, most of the measures concern coordination rather than harmonization.

Prevention and counter-radicalization was in the European Security Strategy and are repeatedly brought up, but there has been very little progress, not least because it is a potentially highly contentious and controversial area. In addition, member states have out of their own individual concerns developed particular programs which they find most useful, and are thus quite reluctant to divert their resources into a common approach. It is also potentially problematic for social cohesion if the recently adopted internal security strategy is implemented as intended, because it calls upon the population to really get involved in information gathering and ultimately data sharing. This is potentially socially divisive; we can talk about the implications of that during the Q&A session.

In terms of internal assistance, yes, common security and defense policy operations have focused much more on the civilian aspect than military components, and are all very much targeted towards promoting rule of law and enhancing capacity in these areas. However, with regard to high-level dialogues with key level countries as well as assistance programs, practitioners have reported little success. This is partly because there are no shared threat perceptions and priorities. The EU sees terrorism as a relatively high priority, but politically in the broader scheme of things, its negotiating partners are not necessarily convinced that they need to assign it an equal level of priority. And there is little connection between the assistance programs and the broader political issues being discussed.

Now some analysts have recommended that increased funding would be a way forward. I do not think increased funding alone would be a way forward; it needs to be tied in with much clearer targets, and a much clearer evaluation of what the funding should actually achieve. It is also argued that it needs to take a much more productive role in the Middle East peace process, a much more constructive relationship with Turkey, and closer cooperation with the North African countries.

So where has the EU gone? There are often clashes between the interests the EU pursues, including the material interest in areas of trade and economic matters. There are very frequent clashes between EU interests and its normative aims of strengthening the shared values in its periphery and further afield. Sometimes conflicting policy also tends to get in the way of success. On the one hand, the EU is the biggest global donor of development aid, and on the other, it has very high access barriers to the EU market.

Internally the EU's problem is that there is a multitude of organizations both in the council and the commission. It is extremely difficult to coordinate them. Because the counterterrorism coordinator has no powers anyway, he often gets to the point of basically concluding, "We know that we need to coordinate, but nobody wants to be coordinated." There has been some success at harmonizing the approach; mainly in the form of the European arrest warrant and definition of terrorism. But overall coordination would be better, as it would be more effective than harmonization.

The bigger picture! Now, the EU's terrorism problem pales in comparison with Pakistan's, counterterrorism or terrorism problem. Nevertheless, the EU does need to bear in mind that that it can also be a source of terrorism, because terrorists, or suspects, have been arrested there. Now of course being very much aware of this, it is trying very hard to add value to national member states' counterterrorism policies. But sometimes its commitment to pursuing these counterterrorism policies and the protection of human rights clash with each other. If technical improvements to sharing of data and information, and facilitating knowledge are to be seriously brought forward, then there is – from a liberties' point of view – also the question of "how can this data sharing be made more efficient without jeopardizing the legal protections for citizens or visitors to the EU?"

More in the context of Britain then in the EU (and I am not going to be able to go into detail but I talk about that in my paper at some length), there is the risk that if we overemphasize counterterrorism, we end up defeating ourselves, because if we privilege security over liberties, we must eventually ask: "If we are trying to defend a democratic society with civil liberties - which is generally seen as a great achievement - but we demonize that, what are we defending?" We are then just engaged in building security while losing the very thing we are trying to protect through this security.

But I want to end on the point of trust – and again, I hope that comes out much more strongly in the paper – the aspect of trust in cooperation and at all levels. Now trust is sometimes seen as something we will build, and eventually come to an agreement; and then we will establish confidence-building measures. This is not so. Trust can only be established if it is a continuous process. There will always be barriers to trust, but if they are overcome in small steps, then hopefully a more coordinated, cooperative approach can gradually be achieved. We must only hope that we have enough time to actually achieve this kind of approach, and implement it effectively. With that extremely fast gallop, I thank you very much for your attention! And I shall hand the podium over to my fellow panelist.

Thank you!

Mr. Ahmer Bilal SOOFI (PAKISTAN)*

"A Perspective From The Sub-Continent"

Chairman,

Ladies and gentlemen,

It looks that I'm the only lawyer in this gathering, in a practitioner sense, and therefore the lawyers have a certain degree of notoriety associated with them. It is alleged that they complicate the obvious first, and then they asked for the fee to simplify the same. I will not try and complicate what I intend to present to you, but I hope that I will try to put it across simply so that we are together on the concerns that we raise, on the very important topic that I have to present to you.

The topic is the role of international law in countering terrorism, a perspective from the sub-continent. So, there are three things that we are talking here. The sub-continent as a territorial entity, the role of international law as a discipline, and how far it can influence the process of counter terrorism. And third, we are looking at the role and the terrorist itself. How this triangle will work together will be the way I will structure my presentation.

For countering terrorism there are three levels. Level one is the conceptual level, level two is the operational level, and level three is the preventive level. And international law has a role to play in each of these levels.

* Ahmer Bilal Soofi is the Senior Partner of a Lahore based Commercial Law Firm. Mr. Soofi has done LLM from the University of Cambridge (UK) and specialized in international law. He has been a fellow at The Hague Academy of International Law, Cambridge Commonwealth Trust, Stimson Center (Washington-US), ACDIS Program University of Illinois, USIS and Private International Law Institute (Rome-Italy). Mr. Soofi has been a consultant to the Federal Law Ministry, Privatization Commission, Ministry of Foreign Affairs, Naval Headquarters, Ministry of Communications and other Government departments. He is Member Legal of the WTO Advisory Group formed by the Ministry of Communications. Mr. Soofi is also on the visiting faculty of the Pakistan Administrative Staff College, Navy War College, Civil Services Academy, International Development Law Institute (Rome-Italy) and Center for Strategic Studies (Sri Lanka). He has also worked as Consultant for the United Nations Commission on International Trade Law (UNCITRAL) in Central Asian States. Mr. Soofi's area of practice is High Court and Supreme Court Litigation, banking and contractual matters and related trade disputes. He is also working as Additional Deputy Prosecutor General, National Accountability Bureau in the current Government.

At a conceptual level we have international law producing treaties, conventions, legal instruments that address issues like definitions, and that address how implementation will be taken up. There are challenges in this area as well, but this is not what my topic would be. So I leave this idea with these respective challenges for the Q&A if required.

At the second level is the operational level. International law again has a direct role to play from an operational point of view for countering terrorism. Through implementation of this vast framework of treaties, instruments and chapter 7 resolutions amongst the states, into the states and then creating obligation for implementing legislation and then those implementing legislation line up with international obligations, creating administrative obligation on people who take decisions within the state. And in doing so when the event of terror happens then within the larger frame of international law and the domestic legislation the stakeholders proceed for the arrest, for the law enforcement and then proceed for prosecution, punishment and other issues relating to due process. Again there are a variety of challenges associated with this level what international law has to play a role. And in the context of sub-continent I will only take the case study of the Mumbai trials. But towards the latter part of my presentation as an evidence of the role that international law can play in terms of bilateral relations, and in terms of handling a transnational crime as well.

And lastly, gentlemen, is the preventive level. Preventive level is where we have to prevent, and the occurrence of the crime of terror not only in a traditional crime law enforcement sense but in a sense of changing the mindset of a terrorist and those who are available to him, and those who are lined up for him. How do we address that mindset in a conceptual framework, and what role the international law has to play in that? How do we influence that dialogue or disclose with religious scholars who have creative perspective of a conceptual framework for those who will be into or attracted to the acts of terror.

I will be focusing on, number three, which is attempting to change the mindset of a terrorist who is motivated by the religion to international law as an international global discipline and therefore my focus is not on a terrorist who has a criminal background, who has a mens rea or a criminal intent, but my focus is on a terrorist who is either persuaded on religious lines and who gets completely betrayed by his own concepts and then he gets things into the act of terror. What I am doing here I have presented a paper to the conference, 24 pages paper, and I am just going to run you through some of the sub-titles of this paper.

The mindset of the terrorist, the highlighting usefulness of adherence to the international law. And again as I said, the mindset of a terrorist in this particular case for the part of this presentation means an individual who has been persuaded on religious motivation factors not on political considerations. Yes, a terrorist group, its had me, have political ambitions. But the way to persuade younger people, the way to persuade people in the villages they normally look up and they normally excite religious motivation factors, so that mindset has been developed within the framework of Muslim Ummah. The mindset gets develop and if your brother anywhere in the world is in trouble you have a right to use forces against the perceived enemy or who will ever serve as a perpetuator irrespective of frontiers, irrespective of legal bars, irrespective of legal framework that exists in the modern world.

Usefulness of adherence to international law needs to be highlighted. And why, because after all adherence to international law is an issue of mutual benefits. As in Pakistan, in Turkey, in India, in US ratify Chicago convention relating to all of flight rights, it is in mutual benefits. While Pakistan international airlines can fly over Turkey, Turkish airlines can use same airspace subject to ratification of bilateral or multilateral instruments, so adherence to international law is in mutual interest.

The objectives of Islam in international law are the same. World peace, progress, progress for the humankind as a whole, because progress is the mandate, and this is the argument that needs to be presented to people who are working in madrashas, who are working in religious scholars and we are looking into any area of Islamic jurisprudence.

Remember sub-continent is the largest territorial venue for the Muslims anywhere in the world. You put together number in India, Pakistan, Bangladesh, Afghanistan if you put it as part of sub-continent as well. We are looking at the largest concentration of Muslims. In India and Pakistan, in particular, the schools of thoughts of Islamic jurisprudence have evolved, and the works of these scholars, these Muslim thinkers are read, and people are nearly get persuaded by that. And it is my suggestion, and it is my also thesis in the last 60 years or so the work coming out of these Deoband Muslim school of thought or Maulana Maududi school of thought, or any of the scholars schools of thought, has no mention of the developments of international law over last 60 years, so if we see this disconnect, on one hand Muslim scholars continue their own discourse, their own discussion and on the other hand international law has been developing as such a fast pace treaty after treaty coming, creating obligations on the state. Each treaty representing a progress being made by mankind, each issue representing certain commitments of the state, more than thirty thousand treaties, multilateral, bilateral instruments, Islamic discourse of Islamic scholars is totally oblivion of these.

If you pick up the writings of any Islamic scholar of standing in the last sixty years whether it is, as I said, Maulana Maududi, whether professor Nike, whether it is from Deoband, whether it is from Jeddah, you will find that not even a single scholars has carried out discussion of an ongoing international developments as something which rhymes with international Is-law, with Islamic Law, and that disconnectness creating a gap in which the terrorist are finding a space. And then which is also surprising because not even a single scholarship mentions that treaty and honoring a treaty is part of the mandate of Islam.

When the state has committed to a bilateral instrument or a multilateral instrument then state is bound. And not only the state, state is after all legal fiction. Individuals of the states are bound, so if you have committed to a non-intervention treaty then the individuals of that states have an obligation to adhere that obligation as well. But who is going to tell this to them? It can be done at a state level, at level of the capital, but in the discourse this needs to be brought out more sharply.

Yes, there is a right to criticize the treaty versus the right to act against treaty which is a very very important distinction. Any Muslim group has a right in Pakistan or in India or in US to protest against a treaty. That no treaty is wrongly done, it is wrongly executed, but no one has a right to act against it. Because once it has been executed, and as we remember, the saying of prophet from which is one of the derivative resources of Islamic law. Even at the cost of disadvantage you have to honor an agreement, and all these multilateral treaties are the agreements that need to be honored. Which is also surprising, because this omission on the part of the Islamic scholars is also noteworthy because on one hand Islam was pioneer of the bases of International law.

I will talk about the proposal little later. Just to give you briefly, there are two milestones. Milestone one, about one thousand years to 1945 we have a one timeframe and then from 1945, from the UN Charter onward still today 2010 we have a second timeframe. These two timeframes have a dramatic change, and we need to understand the Muslim discourse in this context. Before 1945, before the UN Charter the only mold to acquire territory was occupation and aggression. So military might and military aggression was a legitimate mold of acquiring territory. So, during those times the Muslim scholars justified military aggression to claim title to territory which is just fine.

The international law as it then was in 780 in 980, in eleven hundred, in thirteen hundred, the international law also supported this view, was running in parallel to this view. But yes, you can claim title to territories through occupation, and that was the only mold to acquire territory, only multi-material title, so the view of Islamic thinkers in international law as it then was prior to 1947 was moving into the same direction. There was no serious disconnect so you could excite people for the jihad, you could excite people and you could have Iqbal, the famous poet of the east saying that yes you can move on with your armies, cross frontiers, acquire territory and be the great Muslim warrior. But then came 1945 and the UN Charter which drew a red line on most of this thinking process and it said use of force is prohibited in an aggressive war only in self-defense of course. You cannot occupy territory. The war became illegal and all boundary treaties had to be honored by the states and their citizens. All laws meet to implement treaties had to be obeyed by citizens of all states including the Muslim states.

Of course international law has failed on two important occasions in Kashmir and in Palestine that is what major failing has been. But After the UN Charter or the UN Charter treaty provided an insurance to insure that now title will not change hands through occupation. But while the Charter said this, the Muslim scholars continued to move into opposite directions, the thinking process, the entire Muslim discourse of Muslim scholars continued to move in the same momentum. The result was, we are moving now in opposite directions. On one hand is international law, and the UN Charter; on the other hand, on opposite direction are the Muslim scholars' view of having a boundaryless Ummah. And there is a need where international law can play a role is that you have to synthesize these Muslim scholars. You have to bring to their desk to their tables the importance, these texts of these treaties.

I was talking to somebody on lunch, and he said we think Muslims know this. But the fact is Muslim scholars do not know much about it. We, in Pakistan, conducted a small workshop inviting certain religious scholars around the table.

And we distributed amongst them UN Charter and Security Council Resolution 1373. They were shocked. The scholars said: "We thought these were confidential instruments." I said: "No, go through it". And then when they went through it they said "We had been never realized that our individual acts can embarrass the commitments made by the states." So then, to reduce the space, and to eliminate the space for that terrorist to become persuasive, Muslim thinking process, Muslim scholars have to be synthesized with a framework of international law. And as I said earlier not even a single work of any Muslim scholar over the last sixty years in opposed to UN Charter framework creates a synergy but even analyses that treaty framework. So Indian and Pakistani Islamic jurisprudence development has been going into one direction while on the other hand the global discipline identified two treaties has been going into totally in opposite direction. This conflict needs to be resolved, and this conflict can only be resolved if international law is titled as a force, as a discipline brought to the notice in an organized manner. And I have a few suggestions for that as well.

And of course I will skip this slide by merely saying that once you have a religious sentiment but if you are determined to violate international law then you become a non-state actor. Often Muslim scholars failed to understand why the world is after them. Why the world passes resolutions against them, why they are notified on 1373 list or 1267 list. They failed to realize. Not assessing that the game plan, the entire goal post of the global discipline has changed. These are my recommendations. OIC should take up this issue, at an OIC level if there is an awareness campaign to make Muslim scholars aware, the writings will develop that synthesis. Basic international law handbook will be prepared in local languages Urdu, Hindu, Arabic, Persian and Pashto. It should be prepared by OIC and Qatar foundation or any other respected venue and widely circulated in the Muslim World. Wafaqul Madaris in Pakistan and State Madrasa Board in India should be assisted in preparing more detail international curricula which to recommend to religious scholars and religious colleges.

In Border madrasas we approach directly a conference of those Pakistan and Indian scholars be convened. Specific project in Islamic Law and in international law should be carried out in important universities and in Muslim world. A think tank may be considered, and debates in media of Muslim World in this issue should be encouraged.

Now the remaining titles that I wish to discuss I do not have time but just two quick things Mumbai issue. We are coming back to from conceptual framework to the practitioner side. When Mumbai happened it was basically a transnational crime which is committed in Mumbai with allegedly conspired in Pakistan with links over several of the states US, Australia, Italy telephone connections. The trial was supposed to be handled like a crime, was supposed to be handled under the framework of international law, within the framework of mutual legal assistance, within the framework of the international conventions and 1373 mandate to have law enforcement cooperation. Instead, the trial has become so heavily politicalized. That no one is concerned about the legality, but the states Pakistan and India are more concerned from the political perspective. What Indian government did handed over the dossier to Pakistan of so called the evidence which unfortunately turned out to be mostly inadmissible in the court. And as a consequence now we have facing a political situation that needs to be handled. Because if the conviction is not handed out as expected it will have its own political ramifications.

So when politics take over and international law takes a back seat then the outcome will be very very nonproductive. In an issue of this nature where this trial is about to determine the bilateral relations between two nuclear armed states. So, the role of international law in bilateral law enforcement is critical and it should be addressed at that level and at that plain itself.

One last point that I wish to highlight, not all of them, is that the recent phenomena of miscreants being arrested in law enforcement operation in large numbers. What do you with them? How do you handle them? Do you surrender them for anti-terrorism courts or do you handle them in a different mold altogether.

This is a new challenge that at least Pakistan is now confronting that people in large numbers drop weapons whenever law enforcement operations is done in northern part of Pakistan. And then what do you do with them? Because the law enforcement operation is still continuing. Do you pick them up and take them to the nearest anti-terrorism court? Because anti-terrorism regime basically is a peace time regime and here you are having a law enforcement all out action in need of civil power action. So what do you do with that? So there is a need to consider modules from international law and consider their adoption or consider local legislation whether should that be an action in the aid of civil power regime being invoked whereby the courts may consider traveling with the action in the army itself. And wherever there are people who are miscreants they could be taken care of in the framework of due-process and yet it has been enclosed to the evidence itself. And if that is difficult than the framework of the internship for which you retain miscreants or terrorist or who those surrenders needs a lawfull authority behind it.

Under international law again you have a general precedent but within framework of the domestic legislation there that does not exist. So again in this practitioner sense international law will have a role to play in this area. So this was some of the points I wish to highlight. For the rest I can take the questions and answers. Thank you very much.

SECOND SESSION

FUTURE TRENDS IN COUNTERING TERRORISM

Chairman:

Prof. Dr. Faruk BOZOĞLU
Middle East Technical University

Speakers:

BG Murat ÜÇÜNCÜ
Chief of Information System Division,
Turkish General Staff

Prof. Dr. Nils Petter GLEDITSCH
Norwegian University of Science
and Technology

THIS PAGE IS INTENTIONALLY LEFT BLANK

BG Murat ÜÇÜNCÜ (TURKEY)*

"Cyber Defence Challenges And The Importance Of System Management"

Sir,

Distinguished guests,

My speech will cover the Cyber Defence Challenges and the Importance of System Management to tackle the problem of cyber attacks. I would like to start with an interesting story, which happened more than 20 years ago in 1998. A graduate in information sciences, Mr. Morris, who I suppose is currently a Professor at MIT, prepared a software code to prove the deficiencies of the internet and to demonstrate how a worm can be used for cyber crime. What he did was to release a worm in the Internet and then he started to observe the outcome. He was able to receive feedback whenever the code reached a machine. But he was surprised that the worm damaged many more computers than he had expected. Then he decided to send a message to all infected users via e-mailing explaining how the code can be removed from the individual machines, but unfortunately, it was too late, some of the computers had broken down, others could not reach the computer due to security checks.

Overall, more than 6,000 computers were badly damaged, computers in medical institutes, in universities, in military facilities; the reported damage

* Brigadier General Murat Üçüncü graduated from the Kuleli Military High School in 1976 and the Military Academy in 1980. He was transferred to the Department of Electrical and Electronics Engineering at Boğaziçi University in 1980. Upon his graduation in 1983, Brigadier General Üçüncü received his MSc. (1985) and Ph.D. (1989) degrees with his dissertation in system & control sciences from the same university. He taught cadets, undergraduate and graduate students in the Electrical and Electronics Engineering Department of the Military Academy and at several other universities in Ankara from 1989-2003. He worked in the 1018th Heavy Maintenance Depot from 1983-1985, the Department of Electrical and Electronics Engineering of the Military Academy from 1986-1987 and Communication & Information Systems Division at the Turkish General Staff HQs from 1987-1991. He continued his career in NATO HQs (Brussels) by joining the BICES project as a systems engineer from 1992 to 1995. Following this, he returned back to the Information Systems Division at the Turkish General Staff HQs where he worked from 1995-2007 as project officer, head of branch and chief of division. He was promoted to Brigadier General on 04 August 2007 and he still serves as the Chief of the Information Systems Division. Married and a father of one child, Brigadier General Murat Üçüncü speaks English and German fluently.

amounted to almost 100 million dollars. Now, comparing the number of users and computers in 1988 with the current numbers, which has increased up to 1.6 billion online-connected devices to the internet, it is unpredictable how the damage would be today.

Today, the cost of damage due to cyber attacks may go up to trillions of dollars. Let me give you a simple example to illustrate the dimension of the danger. In a case of data theft in June 2008 a former employee in big company, which is selling micro processors, downloaded 1 billion dollars worth of confidential intellectual property documents before leaving the company to join AMD, a competitor of Intel.

Quite unexpectedly and surprisingly there is an inverse relationship between information system security and technological development. It is a sort of paradox.

One of the main cyber threats is malicious code, code that may endanger our whole information system. A big security company, Symantec, identified 1.6 million new malicious code signatures in 2008. The figures for 2009 have not been published, so in my speech I will only refer to the statistics released in 2008. This figure is in fact a 65% increase compared to 2007 when more than 600,000 malicious code signatures were added. When you carefully examine the study and the figures published by Symantec, you find that more than 60% of the total was created in 2008 alone. This in fact tells us that the creation of malicious code in the cyber world is increasing exponentially not linearly.

In addition to malicious code, 75,000 actively infected computers - that is computers, which are not at the disposal of the owner - are reported every day. This is an increase of 31% from the previous year. More than 5,000 vulnerabilities were documented in 2008, which is also almost 20% more than 2007. In addition, Symantec detected almost 60,000 phishing website hosts. Phishing website is trying to steal our visa card numbers, user names, passwords and much critical information. This is also an increase of 66% over the previous year, a very big increase indeed.

The number of internet-connected devices is estimated to be as high as 3 billion by the end of 2013. Moreover, the user population is shifting from West to East. Probably this will result in tomorrow's web to be dominated by a mixture of several languages: English, Mandarin, Chinese, Portuguese, and Russian. In addition, the internet traffic is growing by about 50% annually. We all know that the web has changed the way businesses and consumers communicate and interact with each other. However, web pages are now the fundamentals of malicious activity over the internet. According to reports, there is a dramatic increase in the number and sophistication of web-based threats. 73% of vulnerabilities on the internet are reported to be related to web technologies. It is also interesting to note that 83% of websites have had at least one serious vulnerability and today 64% of websites have at least one serious vulnerability, which may be manipulated by hackers and people with ill intent.

Another threat are mobile technologies that have become dominant. And mobile technology is also being used ever more widely in the military area. Unfortunately, it is very easy to develop malware for mobile devices and – worse still – mobile users are not aware of the threats. Several reports state that thousands of handy devices are lost at airports, a big percentage of lost mobile devices belonging to organizations carry critical information.

Some of the threats I have tried to summarize can also be initiated very easily. The attackers can use a global capability pool, which provides all the necessary software to initiate attacks. The only thing the attacker needs to do is to find only one page, one open door. To defend against the attack, however, we need to close hundreds of doors and we cannot close all the doors because for information systems in order to run we need to open a minimum set of doors. Against these cyber threats, most organizations use more or less the same or similar technologies. We use firewalls, antivirus software and anti-spyware tools. However, it is not enough to spend millions of dollars on security products. It is necessary to guarantee that measures are properly put in place and continuously effective, in fact on a daily basis. For a big organization, it is very important to invest in comprehensive and systematic information security management systems, ideally, based on internationally accepted good security practices such as those embodied in the ISOIEC 27,000 series standards.

The big problem in fighting cyber attacks is the lack of security awareness of the users. Being security aware means that you understand that there is a potential for some people to steal, damage or misuse the data stored on an institution's computer systems and throughout its organization. Therefore, more and better attention must be paid to these assets. Unfortunately, there are still users who “hide” their passwords in places like on the monitor or under the keyboard. A good example, to illustrate the lack of user awareness is results of statistics compiled by the State Planning Agency of Turkey. The statistics show that 50% of internet users do not use any security precautions that 7.9% of users do not even know anything about security tools, and 42% of users use nothing. Therefore, it is essential to implement security awareness programs and persuade all information system users that they must know at least the IT security basics and be able to apply them in order to develop and maintain a secure information system.

Now the challenging issue is how to avoid the damage of cyber attacks. What we should do is to implement a perfect system management. What are the system management elements? They are system deployment, asset management, configuration management, incident management, log management, routine inspections, performance management, release management and a good service desk.

First of all, do we know what we are trying to manage and protect since we are running very, very big and complicated systems? Do we exactly know every piece of our whole system? And are we sure?

Secondly are we sure that we have selected the most suitable hardware and software to protect our systems. Since there are hundreds of different types of tools and different choices, is our model best suited to fight against cyber attacks with these selected tools.

Again, I would like to repeat that system management should be day-to-day administration maintenance and support job, and this is crucial especially for large-scale organizations, which are under constant attack threats. The most important among these threats are patches. Release and patch management is a very well known issue in system management; mostly it is not done correctly, and hence poses a threat to the system. It needs timely and strict compliance; it also requires very good cooperation with the producer of the software. It is in fact a very time consuming and challenging test. In 2009 Microsoft alone released 800 patches. Assuming that it takes half an hour to implement a patch it takes almost 400 hours to implement all the necessary patches, which is a big challenge.

I would like to give another example of what may happen when we do not implement patches correctly, the Conficker worm. It took half an hour to apply the patch itself; however, but those who did not comply suffered a serious damage to their systems. The estimated number of infected computers ranged from 9 to 15 millions. It also impacted several computer networks. It has spread across warships, submarines, hospitals, and destroyed several users connected to this information system, which reside on military sites.

Asset management is another issue, which deserves special care. In the cyber world, we must protect the computer terminals but the switches, servers, many elements other than the computers also store critical information. Now, do we know how many assets are under our control, and what software is installed on the hardware? Therefore, we need to do routine inspection work and the security patch management very carefully.

It is as I said before not enough to take lots of security measures and implement a good system; in addition, the system must be inspected periodically for security. The new vulnerabilities must be detected and the system must be updated with security patches.

Here you see a real test; you see the number of breaches in a local system compared with the result of the previous test period. You see that there is no drastic change in terms of vulnerabilities. That is after you discover the security breaches. Yet the required precautions and patches do not guarantee protection for ever. Only three months later you may face a new group of breaches. Therefore, the breach level is almost constant, even a short time after a hardening process has been finalised.

From this, we can conclude that the information system is like a living organism and always needs special care. Another aspect of vulnerabilities is the inverse relation between intruder knowledge and attack sophistication. The graph shows that the sophistication of internet attacks has increased over time, while the technical knowledge of the average attacker has declined, because the attacker has access to lots of software available on internet to initiate attacks. Therefore, security professionals must be trained in the attack tools.

Today our systems are highly connected and dependent on other systems. There is an increasing demand for collaboration between and across many systems such as shown on the slide. Traditionally each system administrator worked only for his administration's security problems. In the new environment, our systems are threatened either directly by malicious activities or indirectly by the attacks on the systems we are connected to. Therefore, it is not enough to focus only on the local pictures, effective protection requires a global view, and cooperation and data sharing with other organization are imperative.

And today, the defence against cyber attacks has become more easy and effective. In fact close coordination can be established between communication and information systems, people and intelligence institutions. In fact, this is an absolute must in the fight against cyber crime.

As security monitoring gets more complicated the need for data sharing with other organizations and for outsourcing this task to authorized security providers also increased. Security services providers are organizations that collect data from various clients and construct a global risk map and increase awareness, since a single organization cannot collect all the security-related data and correlate the attacks.

In addition to using MSSP as a new concept, it is necessary to establish links among third party organizations that is computer emergency response teams, to increase cooperation and to defend collectively against cyber attacks. For the military it has become necessary to establish cyber commands since cyber space is now a new and additional dimension to land, sea, air and space.

To conclude may talk: The more complex the threats become, the more we have to do the basics really well and establish a solid foundation. Staying aware and on top of new vulnerabilities and ensuring that patches and software are rapidly implemented is crucial, as stated by the CISCO intelligence manager. Increased complexity of the systems and entire new classes of vulnerabilities can combine so that individual vulnerabilities, that may have seemed relatively harmless, can turn into a serious risk factor when combined with other threats.

Thank you very much for your patience.

Prof. Dr. Nils Petter GLEDITSCH (NORWAY)*

"Climate Change, Migration And Terrorism"

Thank you for the generous introduction and thank you for the invitation to speak. I suppose it is a bit ironic that the lecture on climate change should be moved up one day because of a weather problem.

I am not a climate scientist; I come from a background – as you have heard – of conflict study. I will start by just reminding you that the number of ongoing armed conflicts has declined very substantially in the period since the end of the Cold War. This graph distinguishes between internal conflicts, the green area, and interstate conflicts, the blue area, of which there are always relatively few. This graph includes all conflicts down to 25 battle-related casualties a year, and you can see that there has been a slight increase again in the number of conflicts in the last five years.

However, if you look only at conflicts with more than 1,000 battle deaths in a given year there is no increase even in the last five-year period. Of course wars differ greatly in size, and if we look at the 20th century and the number of annual battle deaths we see that the picture is completely dominated by the two World

* Professor Nils Petter GLEDITSCH (citizen of Norway) is a research professor at the International Peace Research Institute of Oslo (PRIO) since 1984. He has been attached to PRIO since 1964. Professor GLEDITSCH is also the editor of the "Journal of Peace Research" and professor (part time) of political science at the Norwegian University of Science and Technology (Trondheim) since 1993. He was also the leader of a working group on environmental factors in civil war at the Centre for the Study of Civil War (CSCW) (2002-2008). Professor Nils Petter GLEDITSCH worked as a university fellow in sociology at the University of Oslo (1973-1975). In addition, he has been a guest researcher on Simulated International Processes Project at the Department of Political Science of the Northwestern University (USA, 1967), Dimensionality of Nations Project at the University of Hawaii (USA, 1969), Institute of World Economy and International Relations (Russia), Russian Academy of Sciences (Moscow, 1994), Center for Peace and Conflict Research (Denmark, 1994). Professor GLEDITSCH was a guest professor in the Department of Peace and Conflict Research at Uppsala University (Sweden) in 1991, 1993 and 1999 and the Graduate Institute of International Studies at the University of Geneva in 2007. Educated in sociology at the University of Oslo with minor degrees in philosophy and economics, Professor Nils Petter GLEDITSCH's graduate studies include sociology, social psychology, and international relations, notably at the University of Michigan. He is a member of the Royal Norwegian Society of Sciences and Letters (Det Kongelige Norske Videnskabers Selskab) and the Norwegian Academy of Science and Letters (Det Norske Videnskabs Akademi). In addition, he won the Lewis F. Richardson lifetime achievement award for conflict research in 2007 and the Mobius Award for Excellence in Research from the Research Council of Norway in 2009.

Wars. So much so that it can be difficult to see what is going on in the period since World War II. If we focus on that period, we see that the number of battle deaths, in other word the severity of war, is dominated by individual wars. The first peak is the Chinese Civil War and then the Korean War. In the second peak we have the Vietnam War, in the third peak the Iran-Iraq War, and the Soviet-Afghanistan War and so on. The encouraging thing is that the peaks are getting lower; so there is a declining trend, which goes all the way back to World War II.

There is a case for saying that we are slowly moving towards a more peaceful world. Now of course this graph refers only to state-based armed conflicts between organized groups at least one of which is the government. There are other forms of violence, many of those can also be shown to be declining most notably genocide and politicide and other forms of what we now call “one-sided violence”; a generic term for state killing of unorganized people. That also peaked in the middle of the 20th century but has been on the decline since then, despite very bloody events in countries like Cambodia and Rwanda.

Now, what about terrorism? Unfortunately the data on terrorism are plagued by a host of different definitions, and by data-gathering problems. This graph is from the world-wide Incident Tracking System. It shows that the number of global fatalities from terrorism, gathered in that database, peaked in 2007. It was driven very largely by the Iraq War. These data have been criticized because they attempted to include the kind of violence seen in the war in Iraq, which would not necessarily be included in counting terrorism fatalities in other conflicts. So if we look at the fatalities in countries of conflict, the green bars, and fatalities from terrorism in countries without conflicts, the blue bars, we can again see that there is a very close relationship between deaths from terrorism and deaths from more conventional armed conflicts.

When climate change turned up on the security agenda, a lot of people made dramatic statements to the effects that this will reverse the trend towards a more peaceful world. In a think-tank report for the Pentagon in 2003, Schwartz and Randall were among the first to raise this issue. UN Secretary General Ban Ki-moon and others have referred to Darfur as the first of many climate wars. The Chair of the Norwegian Nobel Committee argued in awarding the Peace Price to the Intergovernmental Panel on Climate Change (IPCC) and to Al Gore that climate change may induce large-scale migration and lead to greater competition for resources which could lead to wars within and between states.

And finally, President Barack Obama added his judgment that there is little scientific dispute if we do nothing. We will face more droughts, more famine and more mass displacement, all of which will fuel more conflicts for decades. In fact, I will try to show, that it would have been more accurate to say that there is absolutely no scientific consensus on this. Some of these statements have referred specifically to terrorism. For instance, a statement by 11 retired US generals and admirals, broadcast by CNN in 2007 talked about climate change as a threat multiplier for instability and argued that, while the developed world will be better equipped to deal with the effects of climate change, some of the poorest regions will be affected most. And this could potentially pave the way for extremist ideologies and create conditions for terrorism.

Thomas Homer Dickson, a well-known scholar in the field of environmental security, has argued that climate change will help produce the kind of military challenges that are difficult for conventional forces to handle: Genocide, guerrilla attacks, and global terrorism.

When discussing the topic of environmental security, including security consequences of climate change, many use an extended concept of security. And obviously climate change involves so many possible consequences and so much uncertainty that there is a good case for saying there is a security problem in a broad sense. But to go on to say that climate change will lead to more armed conflict, is a different matter. In this area, there is a disconnection between statements by NGOs, politicians, and the think-tank literature on the one hand, and the peer-reviewed research literature on the other.

For the IPCC, the security implications of climate change are not a main issue. In the IPCC third and fourth assessment reports (2001, 2007), which aim at summarizing the peer-reviewed research literature on the causes and consequences of climate change, you will generally find that they rely on dozens, sometimes hundreds, of peer-reviewed research reports on most of their conclusions relating to the natural sciences. When it comes to the social implications, there is much less peer-reviewed literature to draw on, and the conclusions are much more debatable.

When it comes to conflict, there are only scattered references in the IPCC report. Unfortunately, when they do refer to a conflict, their sources tend to be rather flimsy. Back-of-the-envelope calculations about the number of environmental refugees sometimes state a number in the order of 200 million by the middle of the century; a figure that has no very solid backing in any peer-reviewed research. The Stern Review (2006) on the economic effects of climate change also makes only few references to security implications; they tend to rely for those references on the same weak sources the IPCC reports refer to. Since the publication of the Stern Review and the 2007 IPCC assessment report, a peer-reviewed research literature on climate change and conflict has begun to emerge. Unfortunately, I don't have the time here to review the studies individually, but so far they do not provide any robust support for the link between climate change and armed conflict.

Let's take a naïve look at the data and just look at the number of conflicts - the green bars – and deviations from average temperature - the blue line. If I had been a neo-Malthusian scholar talking about these 20 years ago, I could have argued that here are two things going up at the same time, so there's probably a connection. If we extend our perspective to the next 20-year period, we see that the two indicators move in opposite directions. What can we learn from this? Absolutely nothing! But unfortunately, the debate about the social implications of climate change occasionally takes this simplistic form of comparing two time series.

We need to take a step back and look at the main physical consequences of climate change: Events like melting glaciers in Polar Regions, sea level raise, changes in precipitation and increased natural hazards like floods, droughts and hurricanes. Then we need to map the possible pathways to conflict from these physical changes. One of the most prominent ones is the idea that sea level rise will lead to migration and this will lead to conflict in coastal areas. Drought, flood and hurricanes could also lead to migration and into the first causal chain. They could also lead to local research competition and to conflicts without people moving. There is also a line of argument that drought, flood and hurricanes will weaken the state and lead to lower state capacity, and therefore potential rebels will have a greater opportunity for insurgency. For the most part the argument about climate change and conflict is in a sense a strong version of the neo-Malthusian model of resource scarcity leading to conflicts. But the final argument about lower state capacity is what you might call an opportunity model of conflict, which emphasizes the opportunity of insurgents rather than their grievances.

There are many counter arguments to these conflict scenarios. First of all, the link between scarcity and conflict is almost completely limited to case studies. Statistical analyses have not converged on a robust association between scarcity of resources and armed conflict.

Regarding the relationship between migration and conflict, there is some evidence that countries with large refugee populations have more internal armed conflicts. But this is probably the result of the fact that many of the refugees are refugees from conflict areas, and they import the conflict attitudes, the organization and the weapons, so the conflict spreads to the neighbouring country. There is much less evidence that economic migration, of which climate migration is a subset, has the same consequences in terms of conflicts. But this is obviously an area that needs more research.

There are some studies that suggest a connection between natural disasters and conflict. But the strongest effect is for geological disasters, such as volcanic eruptions and tsunamis, which are not caused by human-induced climate change. T causal mechanisms between natural disasters and conflict also need to be clarified. And finally there are some significant exceptions like the Aceh Conflict in Indonesia where the tsunami seems to have led to an end of the conflict, rather than exacerbating it.

There are some useful lessons here in what we may call the 'water wars Literature'. 15 years ago it was very popular to talk about the risk of war over scarce water resources. Some politicians and NGOs referred to wars in the 20th century being caused by oil, to be followed in the next century by wars over water. This literature in fact has moved very significantly from the water war scenario to emphasizing the possibilities for cooperation on water. And in fact it has been very difficult to document that any wars have been specifically about water.

The final criticism of the climate-change-to-conflict scenario is that climate change is generally a slow process. And from this point arises the possibility of adaptation and cooperation rather than armed conflict. There is still much uncertainty also about the science which matters when it comes to the question of adaptation. Recently it was revealed that an estimate had been included in the IPCC report that the Himalayan glaciers might disappear within 35 years. This of course would have presented a major problem because the glaciers act as water reserves in the dry periods. So this might have lead to extensive environmental migration. That estimate has been withdrawn, and now it has been suggested that maybe this will take 350 years rather than 35 years. And of course that difference is very significant in terms of the possibility of adapting to climate change.

What about terrorism specifically? Well terrorists are typically not poor, less educated or more frequently unemployed than the average citizen according to the studies by Alan Krueger. So the scarcity models of conflict are even less suited to predict terrorism than civil war or inter-state war. The argument that climate change must weaken already weak governments is in a sense more plausible. However, climate change would have to be very severe in order to have such an impact on state power. Terrorism-targeted rich countries would hardly be affected by these arguments. In this area there is no research yet.

So what are the priorities? We need to couple the models of climate change much more clearly to models of conflict. We need better data on all forms of violence, one-sided violence, non-state violence, and terrorism. And these data need to be geo-referenced, in other words we need to know not just how much conflict there is within a country but in what areas, what parts of the country there is conflict. Climate change does not vary by national boundaries. Neither does violence. For instance, India may have 6– 8 insurgencies going on at the same time, but it would be ridiculous to say that India is at civil war as a country; there is no national civil war in India. We need to look at the interaction between climate change and the economy, but for all the talk about threat multipliers, there is hardly any research that does this. We need to balance negative effects of climate change against potential positive effects; in some areas there may be more food production rather than less and we need to balance the effects. We need to integrate the consequences of climate change with other economic and social changes such as globalization and urbanization, which are in the long term of course very extensive, and could soak up a lot of the postulated climate migration. We need to calculate the cost of reversing climate change as well. And finally, we need to focus on the most important consequences.

So my conclusions are that the climate change is a security issue in the broad sense, but there is little evidence to date that armed conflict is an important consequence. I think the link between climate change and terrorism so far is mostly window-dressing. Because terrorism is so topical and because terrorism is a real problem as this conference shows it is tempting to drag it into the discussion of climate change too. More research on climate change and conflict is definitely a priority and the IPCC's fifth assessment report expected in 2013 should include conflict.

At the end of my talk, I would like to cite some statistics from the US Department of Health; Alan Krueger says about lifetime risks in the US that your chances of dying from heart disease are 1 in 4, in a motor vehicle accident 1 in 88, from criminal homicide 1 in 240, and from terrorism 1 in 69,000. Of course if terrorists acquire nuclear weapons this could be different. But I tend to regard that as a low probability event and in any case Prof. Allison told us that it is preventable.

The probability of being killed by climate-generated terrorism must be even lower. So would like to conclude by citing Allan Krueger again: "Terrorism, as we have experienced it so far, only matters a big way if we let it matter", and that applies in particular to climate generated terrorism.

Thank you for your attention!

SECOND SESSION
QUESTIONS & ANSWERS

Q: Thank you! **Mark Laity from SHAPE**. I have a question to each of the presenters. With regard to cyber, could I ask your opinion: Do you think that we are more vulnerable to cyber terrorism precisely because a terrorist has fewer infrastructures for us to attack back? I feel that many nations may well; even if they have the capability, have their own vulnerabilities that a terrorist could work. But I am not sure how terrorism would beat the terror. Maybe you could give us a comment on that, please!

A: BG Murat ÜÇÜNCÜ: If I took your question correctly. In order to tackle the problem of cyber attacks as I tried to point out we need to defend first our system and the necessary things we need to do in a timely manner. The terrorists of course facilitate and try to use the cyber arena in order to communicate with each other. It is easy for the terrorists to use the information, system they do not need to spend millions of dollars, and it is easy today, as you know to hire someone thousands of computers, hire them ad try to use them to attack some target whenever the time is appropriate for the attackers that is for a big organization. On the other side we need to spend millions of dollars to implement a big information system and even to maintain a supportive system, we need to pay also almost the same amount of the money that is spent for the investment of the system. But the terrorist does not have such a problem. They can use a small computer allocated being in one nation and they can attack to a target maybe 1,000 – 2,000 miles in a system in another nation. That is very easy for the terrorists; therefore, that is how I understand the problem if I understand your question.

Q: (Mark Laity from SHAPE): To our other guest, well I am sympathetic to your generally skeptical approach. I did rather wonder if you could sort of expand a little bit more on the idea that more evidence is needed with regard to competition for resources. I mean it seems to me that there was life before we have statistical analysis, courtesy of Microsoft. And the number of case studies that there is of competition over resources going back through history which solely suggest that resources are potent source of conflict. Terrorists tend to back know to anything, which is concerned with dissatisfaction, and to exploit conflict does not either trying to do in Afghanistan. So even if the resource issue is not the cause of the terrorism it does create the environment for the terrorists.

A: Prof. Dr. Nils Petter GLEDITSCH: Well, I agree that historically competition for resources has been significant cause of war including competition for territory, particularly competition for territory. But the argument about climate change and conflict is largely framed within the new Malthusian notion that it is scarcity, resource scarcity that leads to conflict. And that is not equally evident, and that's where it has been impossible to find any general relationship in the statistics of this. There have been case studies notably by Thomas Homer Dickson that indicated that resource scarcity is linked to conflicts in developing countries. The problem is with those case studies, here only look at countries in conflict, countries knew that there was a conflict. And then you try to trace relationship between resource scarcity and conflict but many other countries have the parallel resource scarcities but do not have conflicts, then in other words, in order to study the cost of conflict, you also need to look at the peaceful cases and that's what is missing in many of the studies.

Q: GEFC Naples Knowledge Centre Head; regarding cyber defence; as far as I remember one of the slides was on preventive measures or cyber defence challenges. One of them was on the coordination and cooperation with firms, with commercial companies as far as I remember. But I have some concerns about if there are any indications with respect to rivalry between commercial firms in order to denigrate the others' software for example, is there any confirmed information, knowledge, or intelligence about this subject? Thank you!

A: BG Murat ÜÇÜNCÜ: Yes, there are several cases in which some bad software is found in national systems in NATO systems, and system management may be aware of that threat, maybe some time later, sometimes one year, two year later; that is the effect. But the cooperation with companies, if you buy software from companies then you need to have a close relationship. Why, because there are always attacks from people in the cyber arena to try to find some back doors and try to use these back doors in the software to initiate attacks on your information system. In order to tackle such problems you need to stay in contact with the company so that patches will be released by the company. We need these patches as soon as possible so that the back doors cannot be manipulated by attackers. That is a must. We do not have any other way. And we cannot produce all the software in-house, this is not possible for any nation, even for the big producers of software, all companies, and nations are dependent on each other. Therefore, close cooperation with companies is a must in fact. Thank you!

Q: Thank you sir, **Jubi Injava from COE-DAT**. My question is for Brigadier Üçüncü. Sir, thank you very much for your presentation. But increasingly as we move towards automation, there is a lot of industry and infrastructure being run by control system such as Skoda. This would allow a terrorist if he can take over a Skoda system to potentially break things, kill people by having a physical effect through a cyber attack means. Do you think we are concentrating enough on defences for Skoda systems which are primarily network-enabled for patches to be put in? What do you think, is that a vulnerability that a terrorist could exploit?

A: BG Murat ÜÇÜNCÜ: It is not necessary to defend our systems only against the attacks initiated by terrorists. There are hundreds of people in the cyber world who try to attack the system, some of them are just doing this for fun, some of them are trying to receive data from the systems and some of them are terrorist activities. Therefore, we need to take the necessary precautions to tackle this entire multi-faceted problem. Thank you!

THIS PAGE IS INTENTIONALLY LEFT BLANK

THIRD SESSION

TECHNOLOGICAL ADVANCES AND THEIR EFFECTS ON DEFENCE AGAINST TERRORISM

Chairman:

Prof. Dr. Tolga YARMAN
Okan University

Speakers:

Mr. Peter C. W. FLORY
Assistant Secretary General for
Defence Investment, NATO

Prof. Dr. Ekmel ÖZBAY
Bilkent University

THIS PAGE IS INTENTIONALLY LEFT BLANK

Mr. Peter C. W. FLORY (USA)*

"The Role Of The Defence Industry In Countering Terrorism"

Distinguished guests,

Ladies and gentlemen,

It is a great honour for me to be here today to address this extremely distinguished forum on this extremely important and timely topic. And indeed in the face of the global threat of terrorism, cooperation is indeed the only option. That is what we are talking about here this week. It is particularly appropriate that we are addressing the topic in Turkey, a country that has suffered a great deal from terrorism. And NATO stands by Turkey in this battle against terrorism and NATO welcomes and appreciates Turkey's many contributions to the broader Alliance efforts against terrorism from your soldiers and civilians on the ground in Afghanistan, to your sailors' in operation Active Endeavour, where you

* The Assistant Secretary General for Defence Investment is responsible for the promotion of NATO armaments cooperation policies and programs. The ASG is Chairman of NATO's Conference of National Armaments Directors (CNAD) and Chairman of the Board of Directors for NATO's Consultation, Command, and Control Organization. The Defense Investment Division also has responsibilities in the areas of defense against terrorism, intelligence support, airspace management, air and missile defense, and collaboration with non-NATO partner nations. Mr. Flory also is Chairman of the NATO Cyber Defense Management Board. Prior to assuming the position of ASG(DI) in January, 2007, Peter Flory served as the Assistant U.S. Secretary of Defense for International Security Policy. In this capacity, he served as the principal advisor to the Under Secretary of Defense for Policy and the Secretary of Defense on nonproliferation and counterproliferation, security cooperation with nations of Europe, Eurasia, and the North Atlantic Treaty Organization; oversight over the Cooperative Threat Reduction Program and arms control negotiations; and policy for nuclear and advanced non-nuclear deterrent forces, space-related capabilities, and ballistic missile defenses. From July 2001 to August 2005, Mr. Flory served as the Principal Deputy Assistant Secretary of Defense for International Security Affairs, and assisted in the formulation and coordination of international security strategy and policy for East Asia, South Asia, the Middle East and Persian Gulf, Africa, and Latin America. Mr. Flory played a leading role in the development and implementation of Administration strategies for India and Pakistan, and other nations of South Asia. From April 1997 to July 2001, Mr. Flory was Chief Investigative Counsel and Special Counsel to the Senate Select Committee on Intelligence (SSCI). From 1993 until he joined the SSCI staff in 1997, Mr. Flory practiced law with the firm of Hughes, Hubbard & Reed LLP. From 1992 to 1993, Mr. Flory served as Associate Coordinator for Counter-Terrorism in the Department of State with the rank of Deputy Assistant Secretary. From 1989 to 1992, Mr. Flory served as the Special Assistant to the Under Secretary of Defense for Policy. After working as a journalist, he served as a national security advisor to Members of the House Foreign Affairs Committee and Senate Defense Appropriations Subcommittee. An Honors Graduate of McGill University, Mr. Flory received his law degree from Georgetown University Law Center. Mr. Flory also speaks German and French. He and his wife Kathleen have six children.

are the second largest contributor. And of course you host the Centre of Excellence on Defence against Terrorism, our host for this symposium. So we acknowledge and appreciate your country's very important contributions in all these areas. I have been asked to speak about the role of industry in combating terrorism, and I note that my colleague from the panel, Dr. Özbay, will be speaking on a highly detailed and technical topic, in fact, I do not think it could possibly get any more detailed than nanotechnology. Coming from NATO headquarters, General Abu Zaid yesterday covered a broad range of Alliance work in the area of countering terrorism. I'm going to try to approach things from a broader strategic level, beginning with a few words about this strategic picture in NATO.

Some might also note, and they would be correct, an element of self-defence in my choosing the strategic high ground because you all would have noticed my biography, I have nothing like the impressive advanced degrees, specialities and publications of my colleagues in the panel. So, I'm going to go asymmetric on them and not try to compete in their area of expertise.

Now as you know, in NATO we just celebrated our 60th anniversary. Our focus now is on the future, in particular the new strategic concept. Currently a group of experts, led by former US Secretary of State Madeleine K. Albright has been consulting with officials and experts in all our NATO nations, also with our partners in our partner nations, to prepare the ground for drafting a document that will guide and shape our work as we grapple with the complex and challenging future. This new concept will be approved at the NATO summit in Lisbon in November, and as our new Secretary General Anders Fogh Rasmussen said recently "never before has our security environment been so complex, never before has NATO's agenda been so broad. We are going more and more places than ever before. This is why a strategic new concept is so important."

There may be no other area in the world or any other area where the world is dramatically different today from the way it was in the late 90s, when the last strategic concept was prepared, than in the era of terrorism. The old strategic concept was a decent, good document, and it generally had served us well, even though perhaps it is "sell-by day" in terms of events. The old strategic concept was a pre-9/11 document, and while it dealt with terrorism and dealt with the risk of proliferation, it lacked the awareness based on the experience we all gained on 9/11 that certain things are in fact thinkable and that as we meet here thinking about how to prevent them somebody else is meeting somewhere else thinking about how to do them. That is the sense, I think, we lacked prior to the events on September 11.

The earlier strategic concept also predated the terrorist attacks in our own cities, in Istanbul, in Madrid, in London. Again, in many ways the document has served us well, it did not ignore the threats from terrorism, but it did not comprehend the threat as we see today, particularly the linkages between extremism and modern technology. From cell-phones to the internet to possibly nuclear, chemical and biological weapons in the way that Prof. Alison said yesterday, has super-empowered the non-state actor, the terrorist. So we need a new document reflecting current political and military challenges and realities, fit for purpose in the 21st century. And the test of this document will be, in my view, how well we prepare ourselves to grapple with the challenges of terrorism, our strategy, our resilience, our willingness to resource our own security, our strategic communications, which I will be talking about shortly, the critical question of how we work with our own nations, our national governments and with other international organisations - NATO is one of many actors with a role here - and of course how we conduct our military operations, how we develop the capabilities to support our operations.

Terrorism is one of the so-called hybrid threats that Allied Command Transformation (ACT) in its excellent recent study on multiple futures, characterizes as one of the drivers of future changes in the security environment. These hybrid threats represent a combination of multiple factors, placing a premium on organizing and preparing ourselves to maximize our agility and our ability to prevent threats from materializing and minimize our regret factor. Posturing ourselves for this future again will be a key challenge in preparing our strategic concept. So, in this challenging environment where international cooperation is a key factor for success, how could defence industry help? Now, I'm going to interpret here defence industry more broadly than it is generally done to include research and technology entities, academia, think tanks and centres like this one, what I call "the whole cognitive infrastructure", that along with the industrial infrastructure supports our governments and international organisations in dealing with these and other threats.

There are three primary areas where I see we can aim for better cooperation. One is helping understand the challenge, two is providing planning agility, and third is building solutions. In terms of helping understand the challenges, as we have already heard today, and as we will hear later today, we are living in an environment where the threats are increasingly less predictable, or unpredictable in the sense of generating strategic warning because clearly we know that there are those who are actively seeking to attain and use WMD against us, nevertheless difficult to predict in detail or with the timeliness to allow us to prevent them. Terrorists and insurgents employ asymmetric means to attack our vulnerabilities, our lack of agility. So scanning the horizon is a key function and one that the governments cannot do alone.

Defence industry can help us better understand the security environment, trends in technology, and the applications of technology, or perhaps I should say, misapplications of technology as well as help identify new threats and challenges that we may have not even thought about yet. I should point out that NATO was creating a new division at our headquarters, entitled The Division for New Threats and Challenges whose entire purpose will be, at the headquarters level, horizon scanning, understanding the evolving challenges of terrorism, WMD proliferations, cyber-threats and the rest of the litany here. We expect this cross-cutting function to formulize the processes at NATO headquarters to help us better understand how the pieces of this puzzle fit together. This work obviously will fit together with the broad horizon scanning work that is done at ACT.

Now, returning to the role of the industry, our view of technology is often limited on both sides of the equation: the threat side and the respond side. We tend to focus on nuts and bolts or bits-and-bites or thinks that explode, and all for a very good reason. But these are the physical manifestations of technology and such, sometimes do not capture or may underestimate the realm of other expertise particularly in soft sciences, medicals, psychology, sociology, anthropology or economics that has a growing utility for our ability to achieve our objectives. For example yesterday General Başbuğ mentioned the importance of training soldiers in sociology to help them deal with the world with the centre of gravity, which is not the enemy army that we traditionally prepared to go to war against, but the civilian population. And obviously we are not going to war against them; we are going to war to protect them.

In traditional hardware development we need also to engage industry in the early stages of requirement identification. We are in the pre-competitive stages and in this lane we are leveraging the Industrial Advisory Group, the NATO Industrial Advisory Group or NIAG, which conducts pre-feasibility studies in a number of areas of interest including cutting edge technologies, and confirming technical readiness. These studies in industrial expertise help us, NATO, in sorting these questions out. Some of the studies include exploring technologies for monitoring and tracking situation awareness in urban areas, utilizing airborne assets to counter improvised explosive devices, and less specifically focus on terrorism. They are a critical utility in developing our overall capabilities, topics such as heavy lift helicopters, and developing a universal NATO armaments interface.

Now drawing again on the approach of the multiple future studies, we cannot limit ourselves to forecasting or preparing for one single future, hence the title multiple futures. As a famous American baseball player and philosopher once said, "I hate to make predictions especially about the future". That sounds perhaps like a silly point, but he actually had a serious point here, even if he didn't know that at the time. With the multiplicity of the threats and the high regret factor of getting it wrong, we need a broader approach of identifying the key drivers that will shape the future and how we need to prepare for the future. So I see the defence industry as an important partner in this endeavour. The concept of evolving drivers and technology leads us to the next area I would like to focus on, which is providing planning agility. In addition to identifying future threats, organisations such as NATO need to plan on how we will deal with them. Yet to put it delicately, large organisations such as ourselves often do not move as fast as we need to. A successful business model requires innovation and agility to stay ahead of the next idea.

Meanwhile our adversary, we know, is motivated, innovative, decentralized, debureaucratized, resourceful and above all, agile. The Taleban or Al-Qaeda bomb-maker is continually improvising new technical solutions to defeat both our technical counter-measures whether armour or sensors or intelligence collectors or airport scanners as well as social weaknesses, or intellectual weaknesses that they may identify in our countries and in our societies.

So we are planning in a world of deep uncertainty, which is a term that scholars describe as "a situation where the system model and input parameters to the system model are not known or widely agreed on by the stakeholders to the decision." This is not exactly chaos, the word that we used yesterday, but it is certainly a complex situation in which to be trying to plan because of all the variables that we may not understand let alone control. So NATO needs to develop adaptive planning models that strive to combine and match coherently short term requirements with longer term coherent solutions. We have attempted to do this in several programmes, such as in my area of immediate responsibility, the defence against terrorism programme of work focused on the short term, and the longer system analyses and the studies conducted by NATO's research and technology organisation.

However, we must continually re-evaluate our results and pulse our systems and our mechanisms and learn from successful models elsewhere to achieve the agility and flexibility and versatility that we require, which brings us to my third and last topic: the question of building solutions. In many ways this is a return to the more traditional views of the industry's role in building capability solutions. I think there are at least three key elements to keep in mind here. One is, the Alliance relies on nations, and the national industry to develop and apply our technical solutions. Another key point is that the Alliance needs to create an environment where we can work together to identify capability solutions and explore innovative ideas and because we fight as an Alliance and as a coalition, and because many heads are better than one, it is fundamental that we share our ideas, technologies, information and solutions. In an environment like the one we have today where on the one hand we have great threats, but also ever-increasing resource constraints, I hope they will not continue to constrain. I hope that in our strategic concept, as I mentioned earlier, we addressed the question of the need to resource our security adequately. This is something that has been battered somewhat recently or challenged recently by the global economic crisis and that is not surprising. On the other hand, I think a critical element of our strategic concept will be to emerge with the commitment on behalf of all of our nations to resource the capabilities that we need to protect our citizens.

In this environment, however, and it may last longer than I wish, we look at multi-national approaches to building capabilities as an opportunity to share costs, maximize economies of scale, and for many nations to obtain capabilities that they might not otherwise have been able to afford on their own, or that for logistics or other reasons not have made sense for individual countries to pursue in their own individual way, all of which while providing greater inter-operability which is one of the key values, the key capabilities that the Alliance can bring to our many nations. So in short, in many cases such cooperation can be a win-win solution.

Some of this work that we are doing is terrorism-specific, for example, in the defence against terrorism programme that I mentioned earlier. Other programmes support our broader efforts in Afghanistan and Kosovo and Active Endeavour in Somalia. Some, like the Alliance Ground Surveillance System, will support troops in counter-insurgency operations in Afghanistan, but can also help fight piracy or relevant to the threat of technology, particularly the challenges you heard about yesterday from Dr. Alison, and we will hear from Guy Roberts today, the challenges of dealing with terrorism using weapons of mass destruction. One element of such an attack of course is how do you get such a weapon to your target, and our maritime transportation infrastructure is a key element of concern there. How do you, in terms of AGS, do this is a solution that can help us maintain the maritime situation awareness over the sea approaches to our countries that we need if we are going to have a fighting chance of keeping things like this from arriving on our shores.

And industry is of course and will remain a central and key collaborator in this work, even if, I will admit it here, I who presides over many of these activities, that we are not always the easiest customer to deal with. As an organisation with - when I arrived 27 - now 28 heads, our decision-making process and our ability to work with a focused industrial approach is sometimes a challenge. This is why some of our capabilities take longer to develop than they might otherwise. On the other hand, as anybody who has been looking at national attempts to develop capabilities, you will have noticed that nobody has a monopoly on speed in this regard.

So in closing, let me conclude by thanking our host, the Turkish government and Centre of Excellence for hosting this important and timely event and for as always your superb welcome, and your superb hospitality.

Thank you very much and I look forward to answering your questions.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Prof. Dr. Ekmel ÖZBAY (TURKEY)*

"Nanotechnology Today And National Security Applications"

I would like to say welcome to everyone.

First of all, I would like to thank the organising committee for inviting me to present my speech. I was planning on delivering this speech in English, but I heard that the translator speaks better English than me, so I decided to deliver this speech in Turkish. Because of that I apologize to the ones who don't know Turkish. My Turkish is not that good either, I lisp. But hopefully I will not be boring you over the next twenty minutes. I will have three separate sections to my speech.

First of all, I'm going to introduce ourselves, because anybody could have made this speech, you can collect all the information, security, nanotechnology, by searching, but this is not sufficient. What is important from our point of view, what is done in our country, what can be done, what shall be done, these are the questions we have to answer. So, I want to introduce ourselves first, and later on I will talk about what nanotechnology is and how this can be applied in defence applications, especially in security. Then I will talk about what we are doing with

* Professor Ekmel Özbay received his B.S. degree in electrical engineering from the Middle East Technical University in 1987. He received his M.S. and Ph.D. degrees from Stanford University in electrical engineering in 1989 and 1992 and from 1992-1993 he worked as a postdoctoral research associate at Stanford University. Between 1993 and 1995, he worked as a scientist at the US Department of Energy Ames National Laboratory at Iowa State University. He joined Bilkent University (Ankara, Turkey) in 1995, where he is currently a full professor in the Physics Department and in the Department of Electrical and Electronics Engineering. His research at Bilkent University involves nanophotonics, nanometamaterials, nanoelectronics, nanoplasmonics, nanodevices, photonic crystals, GaN/AlGaN MOCVD growth, fabrication and characterization of GaN based devices, and high speed optoelectronics. He is the 1997 recipient of the Adolph Lomb Medal from the Optical Society of America and the 2005 European Union Descartes Science Award. He is also the recipient of 1995 Parlar Foundation Young Scientist, 1996 Tugac Foundation Technology Development, 1997 TUBITAK Young Scientist, 1998 Sedat Simavi Foundation Science and 2006 TUBITAK Science Awards. Professor Özbay is also a topical editor for Optics Letters Journal since 2002 and has become the editor of Photonics and Nanostructures journal since 2006. He has published 230 articles in academic journals and 275 international conference proceedings. He holds 2 patents in the area of photonic crystals. He is currently working as a principal investigator, and executive committee member in 5 EU-FP projects. He is the principal investigator of 10 national projects. After serving as the Turkish national delegate, he is currently acting as an expert in the Program Committee of EU-NMP (nanotechnologies, manufacturing and processes). He is the director of Bilkent Nanotechnology Research Center (NANOTAM) and Bilkent Space Technologies Center (Bil-UZAY). He is a full member of Turkish Academy of Sciences (TÜBA) since 2001.

regard to defence, and what we are doing within the scope of our collaboration with NATO. I always start every speech with my team; I'm just representing them, therefore, I'll put up their pictures. In this context I should like to refer to our founder, who said science can only progress with experimental investigation not through translation. At our centre, which we established, we are trying to adhere this principle.

Of course there is no need to re-invent the things; you can base the new one on existing ones, but if you cannot come up with new technology, you will always be lagging behind. With that idea we reached to a certain point and I am going to try to convey where we are leading to. I carry on with my team, over the past 14-15 years, we have established a centre for 50 people. In fact this team is made up of individuals of different backgrounds and some of these people are PhD investigators, researchers. They are full time researchers, they do nothing else at the university, and in a way because we are an independent research centre, it is the centre that pays their salaries we are directly bounded to the presidency of the university, but we have our own budget. Apart from that, we have professional engineers, we are a research centre but we do applied researches as well. I mean we convert that the technologies that we produce, them into products. We do it with engineers. So it is very important for us to live both engineering culture and science culture. This is our other culture; our students, educating new human resources, coming up with new science is up to this team. It is important to have those two together because if we just do engineering, we are not going to be open to the development. If you just do science, we will never do anything beneficial. We try to keep the balance between these two for 14-15 years. Since we are still at a university and we are educating human resources, it is important. Our students are the primary important products for us.

Dr. Burak Temelkuran, received his PhD from Bilkent University and he was a very successful student. He published 15 articles; this is three times more than what I did for my PhD in Princeton. When I returned to Turkey I said to myself that my students would overtake me, and nearly all of them did. Then Mehmet, who was graduated after, published 18 SCI articles, Burak and Mehmet, they continued their studies at MIT later on. Mehmet is currently an instructor at the university. Then Necmi came up with 19 SCI articles, he has his PhD in Cornell, and he works as a researcher at the university. Then, İbrahim overtook that and now he is a researcher at Carnegie Mellon. İrfan increased the number to 30 his number of articles. He his job was ready for him when he graduated because 30 articles were much more than an instructor writes in his life. How did this happen? These are very good students, these are the best students of Turkey. They came to Bilkent and we made many things possible for them, and they became very good PhD students. İrfan is a researcher at Harvard currently. Of course the rest became very ambitious and Koray increased the number to 34. These are really good figures. I am going to show it in a few minutes later that we can publish 5-10 times more articles than are published under PhD programmes at the best universities of the world. Of course it is hard to keep breaking the records but we have an ongoing researcher, my doctorate student Hümeyra. She increased this number to 32 and she has a two and a half year old son. She managed to carry her career besides mothering her baby. Of course this makes us very proud.

In recent years, we have been publishing an article every ten days. In this present situation we are a research group that publishes the most frequently in Turkey. These are important things as I said , we publish articles in world-renowned magazines like science and nature. Of course it is not sufficient to publish. Does it make your voice heard all over the world? We are Turkey's window opening out into the world. We have been breaking our own record in Turkey. We are referenced so frequently. We renew our Turkey record in the last five years. If we give an example the references in our university are ours; we believe that Bilkent University is really one of the best universities of Turkey, maybe the best. Another example this is the first and the only article published in Science Magazine in Turkey. This is the proof of the well application of basic sciences. This is a record for Turkey. This is the most referenced articles in Turkish Republic history so far and we think that this will keep on being the case for a long time. What we say is invited paper means in every science magazine there is only one. So our academic society it is the crème de la crème. You see that I am a very productive professor and the number of my children is another proof. I always tell with honour that I have five children. I immediately confess that I didn't have them one by one.As you see tose tree who are at the same height are triplets.

Recently, we moved to a new building to improve our research group's project and to have new opportunities. It is a 3.200 m2 new building. I expect everyone. At anytime you like you can visit us at Bilkent. There are different facilities, NANO materials production, and large format production. I won't go into details with NANO integrated equipment but we have all of them. And we use them. We produce large format cameras, Nanophotonic characterization, NANO materials characterization, RF characterization, high frequency circuit characterization. Clean rooms are very important for us, because we have to be free of dust for nanotechnology. Those are examples of clean rooms. Again, Nanolithography equipment. Because with this equipment we have very small dimension pictures of electronic and photonic applications of course. These are the photographs of different applications we accomplished.

When doing this, we always have the application in mind. There are certain organisations in Turkey that we collaborate with. With Aselsan, we have been collaborating with them more than 10 years. Besides military with the civil applications we have been collaborating with Arçelik, Dyo, Tofaş, Coşkunöz Holding and Demirdöküm,. We use R&D (research and develop department) in working systems; we have different patents, different discoveries, and different inventions. Of course these are all within the scope of projects, national security projects come first. We have conducted Ministry of National Defence, and TUBITAK projects. Some are still ongoing. We have resources from the State Planning Agency, also from the EU; we are the centre that is considered as the best with regard to total budget and total number of projects. We are the centre that comes up with the highest number of projects. We try to use this resource productively and I think we are quite successful in it.

Why nanotechnology? Let's start with a striking example: The human brain has a typical capacity of 10 terabyte. So it means, if you have a good computer this corresponds to 20 laptops. If you ask it to a doctor it may change but that is the typical capacity. Whereas today we can write information on one molecule. That means writing information which is 1.000.000 times more than a human's brain capacity in half a glass of water by using NANO technology. That is what nanotechnology makes possible. The first industrial revolution was a "meter, millimetre industry" The steam engine, machine production and industrial automation took place. Microelectronics is the second industrial revolution. While we are getting close to its end the size got smaller 1000 times to one micrometer.

Nanotechnology is the new revolution. This new revolution is on a nanometre scale. It is about to take off now. There are different people from different countries here, from less developed and developing and well-developed countries. What decides where you stand is where are you standing with regard to this revolution. And hopefully we will all be attaining levels of high welfare. I think the biggest reason of terrorism is the inequality of income.

If you ask what is nanotechnology is, we can define it as where quantum mechanic starts, 100 nanometres Its thickness is 1/1000 of a hair. Here, quantum mechanics takes hold, not the rules that we are familiar with. Things that are not possible normally started being possible with those superior characteristics. We can come up with better devices, better systems. How? Thanks to small dimensions of course we have high performance memories, we have high speed, and we have highly resistant substances. We have the materials that can change the colour. And these devices use very little energy. Thanks to these characteristics, nanotechnologies and new technologies when you use them, this can be medicine, pharmacology, whatever, or defence industry, and then we are expecting a new industrial revolution in the future which is not so distant. Today the size of this nanotechnology market is 400 billion USD. Within 5 years we expect it to be 1.6 trillion USD. Many developed countries as you can see are allocating significant budgets. Turkey is lagging behind, but still we have significant resources allocated to nanotechnology all the same.

Nanotechnology is not only used in the defence industry, weapon industry or what we call ICT. Apart from that many technologies are based on nanotechnology. Even today, many things that we currently use are based on nanotechnology. You see a list here. In fact, nanotechnology is on its way full throttle and we have to catch up with it. If we give examples for current applications: Sports rackets, sports technologies, textiles, goggles, glasses which cleans themselves, cosmetics. These are all based on nanotechnology. For the future, new products using sensor technology are on their way. Again, we can write information on one molecule. You see the pictures I got from IBM projects, we can write this by using AFM but we need 10.000 of it to write and read so much information.

Now, if we talk about what we do. Basically we change the electromagnetic properties of the substances. For example, we can reverse and break the light on a substance, and we call it negative index you remember it from your high school physics lesson. When you come up with such a device, an optic microscope, its resolution can be infinite. Even though you can see anything with the microscope this will make it possible. Its another feature is, we reduce the wavelength of light 100-fold, so we focus the light on one tiny point, with the practical consequence that a typical DVD capacity can be increased 100-fold. Another important application is camouflage; you can produce an invisibility cloak. When we talk about invisibility cloak the first thing that comes into mind is to place a camera behind and reflect the vision front, but it is ridicules. To attain real invisibility is a standard optic problem. When light hits an object, it is scattered. As you know, a black object does not reflect light, but it still has a shadow. So the important thing is to design something without a shadow and which does not reflect the light back. This is basically a standard optic problem. But the basic thing here is the electromagnetic characteristics of the material can take on any characteristics in the space. Metamaterials can make this possible and we did it and our current activity is to have that with different colours at the same time.

About meta-materials, our research within the scope of a European project has received an award. In 2005 we were presented the Descartes award. This is the photograph with the Science Minister, the one and only Descartes award Turkey got.

If we go on Nanophotonic, meta-materials, their photonic applications can be seen here. We can make LED an outstanding material. When you merge nanoplasmonic, metallic structures with organic materials, NANO or LED, NANO light source can be formed. This has been published in the Nanotechnology Journal. Our current aim is to have very small lasers with them. Where are we leading to? To the missile warning system. We know that a 500 $ missile can bring down a plane which is one in 30.000 flying all around the world and we have been talking about the crises that it will create for two days. How do we prevent from? You can prevent from this with a missile warning system by catching its light in advance. The current method used is this. It is obstructed by the sun which is very shiny, so it is not possible for this missile to be seen with the naked eye. Because of the ozone layer, the rest of the signals don’t reach the land. The shiniest part of the missile, the UV light which is emitted from there, has to be detected from really far. We have developed a NANO-sensor that makes this possible. We produce millions of these and we made a new camera. Then we have produced this as a package in our centre. As you see we have developed the missile warning system in the university lab. Now you see some pictures of the new generation missile warning system.

Our studies go on by using NANO photonic methods; these types of sensors to make them more selective and we will be using them as thermal cameras. We study on NANO sensors to detect. Biological agents and chemical explosives. We succeeded to make biological sensors with the technology we published in “Science” journal. Again, with the new technology we have an ongoing biological sensors project. Maybe more importantly THC waves are used to detect explosives and weapons on people. The human body does not emit the light but clothes do, if you have a hidden explosive or a weapon this will be detected from 100 metres. More importantly, what sort of an explosive it is, will be identifiable with this method. This is the new project. The whole world is working on that.

If you ask where NANO technology comes from, to create that telehertz waves and sense we need NANO photonic light sources and detectors. Again there are some more studies we have been doing at Bilkent, and here are some examples. We constructed a high sensitive detector. Now it is a produced material. Laser is used in measuring the distances. We are producing high-power lasers, in another subsystem which is used in military. We are working on Graphen as well. This is a great new NANO material. It is a high-power RF material. Where silicon technology ends Graphen will take over. We have produced Graphen NANO transistors at Bilkent within the scope of a European project. We will start on 1st April. High-power NANO transistors; this material works at high temperatures. It is the most powerful material for space. This RF is a circuit produced at our centre.

Where will we use it? Within the scope of this project, as helicopter material plus in new generation jammers, especially for remote control bombs to demolish at least. Even if they are not totally destroying these systems will become effective. Space is important for all of us, especially with regard to observation. Of course for space to be cheap, everything has to be reduced in size. That is where nanotechnology comes in. The biggest R&D project of Turkey has given a way for this with Aselsan. Here, for the first time, a satellite subsystem will be produced in Turkey. Many firsts will be achieved for Turkey.

From our point of view this project is maybe the first Garnitrat based RF chipped model will be sent into space in 2015. Again, I want to end with a quotation from our founder. We are doing many technical things and will continue to do so. I would like to thank all government organisations and EU who have given that opportunity.

Thank you.

THIRD SESSION
QUESTIONS AND ANSWERS

Q: General Babekar Bedirhan ZEBARI: As I have listened to the presentation here, concerning the studies that have been carried out, it was stated that in the work of some countries, he pointed that there were certain weak points. Terrorists and terror organisations are making use of these weak points. Yes, can everyone hear the interpretation? Professor Peter, in his presentation pointed out that the terror organisations and during the research they carried out, they determined the weak points of each country. In order to overcome this gap, it is obligatory to undertake international cooperation. Because the terror organisations, in order to survive, are recruiting new support and they are sort of attracting the young people to their side. They are attracting these young people for their purpose. The terrorists and the terror organisations, we all know very well, provide a great deal of training to their members. The countries by themselves in an isolated manner cannot possibly be successful in combating terrorism. So cooperation is naturally unavoidable. Under the leadership of NATO, and in the work the NATO is carrying out as a counter-terrorist activity, we should support them. And under the umbrella of NATO, it is better and it is necessary, I believe, to work in a more expanded area. I know that this has been a rather long question.

Q: Prof. Yonah ALEXANDER: Thank you very much. I have a question to the secretary, or Mr Flory. I certainly want to acknowledge the contributions of NATO to the global security concerns and obviously you made rich remarks in your overview. If I may, I would like to ask if you could elaborate some of the issues that you mentioned and perhaps make some comments on others. You mentioned the challenge in the maritime environment, could you also mention some of the current activities of NATO regarding piracy. The second challenge is the energy, infrastructure security issue. The third one is the cyber challenge that we discussed about. The fourth is narcotics and obviously on each and every one we can have a special conference. Aside from that, we will hear from Guy Roberts today as well on the challenge of weapons of mass destruction. Finally since we are trying to underscore the significance of partnership, could you tell us a little bit about the plans for deeper partnerships, for example, in countries like North Africa and Latin America. Thank you very much.

A: Mr. Peter C.W. FLORY: Thank you very much. With respect to the initial question, when I referred to weak points, I am speaking about from the perspective of people who would exploit. We generally consider good things about our societies. So, from the terrorist perspective, their weak points... there are things they may aim at, there are holes in the armour they seek to get through. But I am talking about things like our respect for civil liberties which affects our ability to intercept and read communications. It is not that governments don't do this, but our governments do this in ways that are bounded by law and frankly in some cases those laws can make it easier for terrorists to do the things they wanted to without being detected: Freedom of movement. Our concern about privacy, I mean one of the big issues now coming out of the Christmas have failed happily the underwear bomber attack is the debate now over scanners and privacy. We saw some of them in the professor's presentation. But clearly I don't happen to think these are more weaknesses on our behalf, but they are things that provide opportunities for terrorists to do what they want to do and avoid detection and otherwise they further carry out their plans. In terms of dealing with these, we need broader cooperation, as the speaker indicated, in many ways. One of which is, in certain areas, maybe looking at the way we do business and asking ourselves, are those ways of doing business still the appropriate ways of doing business in a different era. In an era where we are dealing with threats and challenges we didn't have before. I think in most cases involved civil liberties and privacy things like that, we tend to come back and say yes, we think it is important to maintain principles. They are after all the principles that define us as nations.

But I think individual nations, certainly with the US, in the aftermath of September 11th grappled long and hard with questions as where is the right balance, where do we need to change the balance, how do we need to do a better job of balancing the rights of our citizens, to include the very important right of our citizens and not to be murdered. So, that is a part of the discussion and I think that something that is... we are not going to get satisfactory solutions if we don't address those and very much with international concept, because if you get a split, a diversion between national approaches, first it is going to create another hole in the armour and secondly it is going to be politically controversial and make it difficult for us to maintain the political solidarity that we need. With regard to Professor Alexander's question, we could indeed have a series of conferences and as much as I enjoy being here in Turkey, I would certainly propose I'd be happy to come back 5 or 6 times to do that. Just quickly on a couple of areas in terms of maritime awareness... NATO has a terrific history of maritime situation awareness based on our Cold War experience: the experience which we have recently been able to put back to good use in operating of the coast of Somalia. Our naval forces did not have to learn... they had to learn some new things but they did not have to learn how to operate together, they did not have to learn how to communicate together, they are the most inter-operable, I have heard say, of all our forces. But the challenge of knowing what is out there, which is the situation awareness, whether as applied to piracy or as applied to illegal immigration or even more threatening possible smuggling of WMD to our harbours in cities. The information, the collection and management of information is critical. And this challenge hasn't changed much since the wars of the early 19th century where British ships ringed the continent just in eyesight of each other with signal flags to announce that particular ships are coming out of port in the particular city and using signal flags that information could travel hundreds and hundreds of miles in a matter of minutes. We have gotten beyond the technology but the basic challenge remains the same. When you are talking about the sea of course, you are talking about huge amounts of areas. That is one of the reasons I'm very excited about the utility of AGS system, when we get that online to adding to our ability. Many of our nations have concerns, many of which involve trafficking of illegal cargos across the Mediterranean, also in the high North. In terms of partnerships, we are working very hard for a number of years to broaden and deepen our partnership. We have in some areas been more successful and broadening it and deepening it. As we have expanded the map of our relationship outward, finding the activities that are most useful and helpful to our partner countries and to ourselves takes time. But you mentioned specifically, North Africa. A number of North African countries are the members of the Mediterranean Dialogue. I had the opportunity to speak to Algerian colleague yesterday about a trip that I hoped to take to Algeria by a year ago which I hope to be able to re-do the talk about the very useful work on Algerian scientists are doing with our research and technology organisation. On South America I have less personal involvement but I would like to point out that Columbia is now a true contributing nation of ISAF.

FOURTH SESSION

THE ROLE OF STRATEGIC COMMUNICATION IN COUNTERING TERRORISM

Chairman:

Mr. Ercan ÇİTLİOĞLU
Bahçeşehir University

Speakers:

Mr. Mark LAITY
Chief of Strategic Communications
SHAPE, NATO

Prof. Dr. Steven R. CORMAN
Arizona State University

Dr. Itamara V. LOCHARD
Tufts University,
Fletcher School of Law and Diplomacy

THIS PAGE IS INTENTIONALLY LEFT BLANK

Mr. Mark LAITY (UK) *

"Strategic Communication Models"

Good morning.

Let me start with a quote, "We are in a battle, and more than half of this battle is in the battlefield of the media. We are in a media battle in a race for the hearts and minds of our Ummah." It is a quote from Ayman Al-Zawahiri to Al-Zarqawi, the latter now fortunately dead. So that is one of the leading terrorists operating in the world today, putting his finger on the heart of the matter, "the media battle in the race for the hearts and minds. The section that I lead has a motto, "Perception becomes reality." Not perception is reality, but perception becomes reality. Because if you think that something is so, you would tend to behave in ways that make it so – a kind of self-fulfilling prophecy. That is at the heart of what terrorism is about. It is playing mind-games. It is the powerless, or people with little power, trying to be powerful.

* Since January 2004 Mark Laity has been Special Adviser on Strategic Communications to NATO's Supreme Allied Commander Europe (SACEUR), as well as a Senior Research Fellow in the Centre for Defence Studies at King's College London. His latest jobs followed nearly four years as Deputy Spokesman and Personal Adviser to the Secretary General of NATO, Lord Robertson. In that time he was involved in many roles in both the policy and media fields. From May 2000 until April 2001 he spent almost a year as acting NATO spokesman. In May 2001 he was sent by the Secretary General to the Former Yugoslav Republic of Macedonia . Initially, he worked as an adviser to President Trajkovski - a mark of the close personal co-operation and friendship between the Secretary General and the President. Then in September, as the deployment of Task Force Harvest raised NATO's media profile, he became the civilian spokesman for the highly successful Operation Essential Harvest - making him a familiar face to many. He was also media adviser to Major General Gunnar Lange, the operational commander and Senior Military Representative. Then he returned to his normal duties in Brussels, where he has had an oversight of NATO's media operations in the Balkans, which have given him the opportunity to make several further visits to Skopje. Mark Laity joined NATO after 11 years as the BBC's Defence Correspondent from 1989, covering all aspects of British and international defence, including extensive experience of frontline reporting, notably in the Balkans. He covered most major conflicts of the nineties, but particularly the break-up of Yugoslavia. Between 1992 and 1998 he regularly reported from the frontline in Bosnia and Croatia, during much of the worst of the fighting. He also reported from Albania and Kosovo. In 1999 he covered the air campaign from NATO HQ in Brussels, before reporting from Kosovo itself after KFOR entered. During this time he became a familiar face worldwide on BBC television. He had fulfilled a similar role with his reports and analysis during the Gulf War in 1990-91, when he was based in Saudi Arabia throughout the conflict, and became an ever-present voice on BBC radio. Mark was born in Truro, Cornwall, and has a BA (Hons) and MA from the University of York. He is now a regular speaker to a range of international groups on military and media issues. Aged 47, and married, he is a keen sailor. Other interests include military, aviation and maritime history.

It is easy to forget that the phrase terrorism is not “kill-ism”. It is terror-ism. It is to terrorize. And you are only terrorised if you think you should be terrorized. So when you break terrorism down, their power is really the power that we give them. An action that they carry out is magnified through publicising it, and in this way information is used to affect our minds, and so change our behaviour. But the acts are invariably small - the people who magnify them are us. So terrorism is information at its purest. It is the primacy of information as a weapon. And the prime part of that information is fear. So it is very clear that we should say right at the beginning: if fear is their weapon, then taking away fear must be our primary counter. We should be trying to minimize fear. In the face of their actions we should be responding routinely, being realistic and determined.

If there is one lesson that we should all learn right from the beginning is that the more we talk about them the more we do their work for them. And one of the major mistakes that we have been making for many many years now is to do their work for them by talking about one terrorist organisation like some figure out of a James Bond movie where its tentacles are everywhere. We have been complicit in creating the fear that is at the heart of their strategy, but what fear is about,and fear is in the mind. However fear alone does not account for why they could be successful. Support for terrorism uses fear, but it is not totally dependent on it. It needs a soil in which to grow. The soil in which terrorism or insurgency - and insurgency is very similar to terrorism in many many respects -and one could have a big legal debate about what it is. It is dissatisfaction with the current system, alienation from current rulers, a belief that it is legitimate to break the law of your state or your society, or international law, in order to achieve your ends.

So if we are to defeat terrorism, we must also attack the roots of the dissatisfaction, of alienation, of a belief that people can only get what they think they deserve by these acts. But why are terrorists often so good at using information? Primarily they are effective because it is their priority, it is what they must do to have any chance of success. They know that if they are not good with information, they fail. So in the same way, as armies are good with weapons but maybe not so good with information, because using weapons us what we do, terrorists are good with information. But we are also living in an era which puts challenges to us and makes life so much easier for them. In particular, we are in the information age. The era of what one can call “the democratization of the media” where everybody can not only say what they think but find an outlet to say and demand to be heard. That is what the internet does. It opens up everything to everyone. In many ways, this is one of the most liberating acts of our age. The information age is in so many ways so good. But of course, if something is open to everyone it is open to bad people as well as good people, evil people as well as ordinary people. The information age now means that it is easy; it is cheap for anyone to use information. We have lost control of our monopoly of managed information.

And of course in the media space which existed long before the internet, bad news for us is in journalistic terms good news for them. Good news in the sense that the explosion will make the news. No explosion, no news. Preventing terrorism means something hasn't happened and so cannot be reported, but a successful terrorist act can be reported and inevitably gives them the publicity they seek. But they also have other advantages. The environment does favour them; they have simple stories, simply told. They tell the world 'they', the government, are bad, 'we' are good, we can solve your problem – everything is black and white. The terrorists also have simple structures which they flexibly use. Terrorists do not have big bureaucracies, we do. And also they deal with the immediate. You, they tell the unhappy and aggrieved, feel angry now, I can give you a solution now – no need to wait. Our solutions are long term. We say "Calm down, wait let's discuss it." And as the anger grows, the willingness to hear our calmness reduces. So we live in an age of instant gratification. The terrorists provide it. How do we respond? Well, that answer is many-sided, but I will look in in particular is what we are doing with regard to information. First we have recently created the concept of strategic communications, which in itself is an acknowledgement of a kind of failure. Our existing way of handling information had not succeeded. Too slow, too complicated, too confused. We needed a new approach. What we are now trying to do in NATO and at SHAPE, using ACO Directive 95-2, is not just to rebrand how we do information with a new title, but to change how we do it more fundamentally.

This includes putting more focus on unity of effort, we have had public affairs, we had the information operations, and we have psychological operations. Very often, they do not work together, and if you push them to do so, they often work against each other with formal coordination but reality institutional rivalries. That won't do anymore. You might have got away with this in a cold war, you might have survived in a hot conventional war, but in the world of terrorism and counter insurgency, where information, as General McChrystal has recently said, is the decisive effort, then you have got to get your information strategy right. So, firstly we need unity of effort and a commitment to pull together, but also to produce an outcome. Strategic Communication is not just giving out information; it is using information to help achieve mission success. And it is also fully integrating information with other parts of the overall effort.

Too often in the past, what we did was first decide our policy and then we pulled in the media chief and said, “Here is the policy, now go and tell people about it”. That will not do – information is too important to be no more than an afterthought once everything is decided. Now, what do we do about it? The intent now is for information to integrated in all aspects of policy, planning and execution. That is reflected in ACO Directive 95-2. So, a few quotes: “Such is the importance of information in mission success than on occasion policies and actions will even need to be adapted and respond to the imperatives of strategic communications.” In the bland bureaucratic prose, there is something quite revolutionary there. It is saying if the message is not working, you do not shoot the messenger, you look at the message, and maybe you change it, which means changing the policy. Such is the importance of information that the message and the ability to selling the policy to our audiences drive the policy itself. In effect we are saying, “If you can persuade people to back your policy it is good, but if you cannot persuade them that they should go with it, and support it, and then you need to change the policy.” Another quote from 95-2: “All HQs must remain flexible and open and adaptive to potential requirements for reorganisation or structural change, driven by areas such as advances and social media.” In other words we are saying, don’t force information management to adapt to our traditional bureaucracy and hierarchy; instead we should consider changing to adapt to the information age. Because what we have with the information age, with terrorism, with insurgency is a challenge to our structures and to our mindset.

Of course there are also old principles of information handling that haven’t changed: credibility and speed. But even here it has got harder. Once upon a time at the strategic level at least, you had time to work things out; no longer. Whether you are operating on a strategic or a tactical level, the information age means you have no time. You cannot afford any decisions, any considerations, any proposals to crawl up from the sergeant to lieutenant to the captain to the major and so on. We don’t have that kind of time when our opponents and the media with their simple one-stop shop responses can move so fast. So we cannot afford the multi-layered structures, which we have loved for so long.

In information terms the tactical or strategic divide is also gone. Tactical actions have strategic effects. Once upon a time the death of a soldier meant nothing in strategic terms. Just another number. Now, the death of an individual can shake governments. So that divide is gone. There are no boundaries, and our organisation has to reflect them. So, we have a fundamental information age challenge to our command and control. I refer to it as abandoning "the delusion of control for the reality of influence". We no longer control the landscape in which we operate. Within our armies we may think we do, our generals speak to their aides and send their messages and everyone click their heels and salutes. But outside our armies, we are not in charge, we are just influencers. We are just another person on the marketplace, shouting along with many other market traders.

Part of the significance of this is that when it comes to information handling we are organised for control not influence. If you believe you can control something, you organize in a certain way. We have to accept the reality of influence, not control. For this you organize differently, and we need to organize differently. We have to accept that we are in an era that we influence, not control. That also means that our words and actions have to be interactive. It is no good planning, acting, and then deciding what you are going to say about it afterwards. You have to say what you are going to do as you are doing it. We have to be more flexible. We must have flexibility versus rigidity. We are in the era where we really have to put mission command into effect. Everyone talks about mission command, but it is so rarely done. In the information age, mission command really is the only way to go. We have to engage not just inform. We are used to having a situation where we control the means of communication whether it is a newspaper, radio or television. We speak; they watch, listen or read. But now, they can speak back. And we must listen. One of our speakers will talk more about this, so I will say very little more other than we have moved into an era of interactivity, where unless we listen and adapt and respond, then we will fail. Because our audiences expect to be listened to, and what's more they expect to be heeded. The directive nature of information handling is no longer effective.

The need to deal with this is highlighted in ACO 95-2 which lays out the need for Allied Command Operations to transition from a 'one to many' posture, towards a 'many to many' engagement approach. Effective communication requires interaction, highlighting the need to listen as well as speak. We need to move to all-inform. It is no longer 'need to know'; it is 'need not to know'. This will give us information handling problems. But when you have the kind of situations we so often face we must move quickly and the multiple layers which tend to create hierarchies and stovepipes will cause us more problems than we can cope with. So stove piping out, all-inform in. And we need Communities of Interest approach. In such a flexible complex environment who really knows for sure who else needs to be involved? Very often a person who is not told is actually important, and if we don't tell them, how can they help us? So again, a challenge to our hierarchies. We need a network approach, a community of interest approach. And this requires empowerment and flexibility, and also willingness to accept mistakes. When you start involving more people, when you start empowering more people, when you start allowing more people to get engaged, things go wrong. So a critical part of dealing with the new environment is to accept mistakes.

Also with the audiences we are dealing and engaging with, we have to put the emphasis on narrative and culture. It is no longer enough to message with pure facts or argumentation and no proper context. This is too often what we are doing. It is time to recognize that what works with people is something that is tuned to their culture, to their story. Too many of our messages tend to reflect what we think they should think. This is a fundamental problem. We need to tune what we are saying to understand how our audiences think, to understand what they want, to understand their story and tune ourselves accordingly. And again, another of our speakers will look at narrative in more depth. But one of the fundamental reasons why we have failed so much in our strategic communication efforts when it comes to those influences by terrorism, was, that we do not understand their culture, and as a result we do not create a narrative that resonates. We tell them what works with us, not what works with them, and we do not listen to them and adapt ourselves accordingly. So we have a massive challenge. We are at least making some progress, I believe. Things are changing.

Finally, when General McChrystal talks about communication as a decisive effort, he is putting strategic communication where it needs to be, where it has not previously been. But to do that successfully, we need to look at our structures more fundamentally. This is not just a question of doing what we have done better, it is doing it differently. And that requires a more holistic approach to everything we do, to all our hierarchies, to all our bureaucracies. That will require training and education to produce new attitudes. What we need to do to succeed is not just to have right on our side, which we do; but to be able to persuade people that we have right on our side. For that we need a new mindset. A perception mindset. And if we have that, I believe we will succeed. Thank you.

Prof. Dr. Steven R. CORMAN (USA)*

"The Role of Narrative in Strategic Communication"

Ladies and gentlemen,

Good morning. Let me begin by thanking the staff of the Centre of Excellence for Defence against Terrorism for inviting me here to speak to you today, and for their very excellent hospitality. Three years ago, my colleagues at the Consortium for Strategic Communication published a widely read paper entitled "A 21st Century Model for Strategic Communication in the War of Ideas". In that paper, we argued that the current strategic communication practice in the United States and other countries is based on the 60-year-old idea of how communication works. This model is actually based on a model of telephone systems developed in the 1940s by an engineer named Claude Shannon. He described the elements of the telephone systems in order to indicate places where it could possibly fail.

Now, Shannon drew a box and arrow diagram, but I thought I would improve it for you with some high quality professional graphics. So here, we see the person on the left is saying something into a telephone receiver. The telephone receiver translates his voice into an electrical signal which is transmitted over the wires. During transmission, it may be interfered with by noise and it arrives at the receiver at the other end where it is translated back into sound that can be heard by the

* Professor Steven R. Corman has directed the Consortium for Strategic Communication at the Hugh Downs School of Communication at Arizona State University since 2002. He is the coeditor of Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism, and served on the scientific panel for the Strategic Operations Working Group at the US Special Operations Command from 2005-2006. Most recently, Professor Corman received the International Communication Association's Outstanding Applied Public Policy Award for his work in communications as a counterterrorism tactic. Professor Corman has also served on the editorial board for the Journal of Communication, the Management Communication Quarterly, and Progress in Communication Science. He has served in numerous national and international workshops and symposia on counterterrorism, strategic communication and public diplomacy and worked at the Informatics Faculty of the Karlsruhe University (Fakultät für Informatik, Universität Karlsruhe-Germany) in 2003 as a visiting professor. Professor Corman's academic credentials include a B.S. in communication from the Illinois State University, and both an M.A. and Ph.D. in communication and communication theory from the University of Illinois at Urbana-Champaign in 1994 and 1988. Prior to receiving his associate professor and assistant professor titles at the Arizona State University, Professor Corman worked at the Department of Speech Communication at the University of Illinois at Urbana-Champaign as a teaching assistant and research assistant.

receiver. So this is Shannon's model of telephone systems. In the late 1950s, a person from my field named David Berlo used Shannon's model of telephone systems as the basis for a model of human communication. And to give you an idea of just how old this model is, I thought I would show you a graphic that Berlo used. It is shown here.

So, on the left is a source which has attributes like communication skills, attitudes and so on. The source formulates a message that is represented by the second box. That message is transmitted by any number of channels like sight, sound, touch and so forth in the third box. And it has a receiver on the other end that has a similar set of attributes to the source. Hopefully the similarity with Shannon's model of the telephone system is obvious here. So, Berlo wrote a book based on this model that was used in training for the US State Department and in college classes throughout the 1960s and 1970s. As a result, his model of communication became the basis for practice in a number of fields like communication, political science, marketing, advertising and so on.

Now in our paper we showed that this is still the dominant communication model in strategic communication in the US and other countries even today. If you accept Berlo's view of communication, then it has an important implication. First, communication involves sending signals or messages to a well-defined audience as if they are being transmitted over the telephone system. Messages arrive fully formed at the receiver and influence the receiver in that way. The main constraint on the process is the skill of the sender in formulating and transmitting messages. Communication fails when the message does not get through clearly, either because of noise or misunderstanding. A corollary of this is that communication can be expected to succeed unless something goes wrong and prevents it from succeeding such as the noise.

Finally, certain best practices, like repetition of the message can help ensure that communication does not fail. But as we showed in our paper, communication theories since the 1950s have moved on to a more complex model, that we call "pragmatic complexity". In this model, communication is no longer the transmission of messages from source to receiver, but instead a simultaneous ongoing dialogue between participants. In the interest of time, I will not go through all the details of this new model, and instead refer you to our original paper if you are interested. But one key aspect of this model is context in which the ongoing dialogue operates. It includes things like history of the relationship between the parties, other dialogues that may be going on between other participants at the same time, changing social and cultural meanings for the symbols used in the exchange, and also the narrative on which it draws. That brings me to the subject of today's talk: narrative.

My colleagues and I are currently working on a grand project to study extremists' use of narratives in contested populations in Southeast Asia, Southern Europe and North Africa and the Middle East. In this project, we make a distinction between story and narrative. A story is an account of a sequence of events. So for example, "Prof. Corman travelled to Ankara. He went there to give a talk at a NATO Terrorism Conference. His talk discussed the importance of narrative and strategic communication." This is a story. A narrative, on the other hand, is a system of stories. So we might say that all of the stories that the organisers and everyone and all of you, everyone who came here today create a narrative of this symposium.

There are two important points I would like to make about narratives. The first is that they provide a frame for understanding what is happening and what people are doing in a given situation. Take for example the preface written by Colonel Özkürkçü in the activity guide for this conference that you all received in your packets. In that preface, he tells the story of the 9/11 attacks in the United States and challenges in military strategy and international cooperation that this has brought about. He then tells the story of the Centre of Excellence Defence Against Terrorism, and what they have been doing to meet these challenges. In doing this, he invites us to understand what we have been doing here for the past two days as a part of that larger effort, as part of that story. In other words, this system of related stories creates a narrative which provides us a frame for the symposium. The extremists use the narrative in the same way to encourage their audiences, to make sense of what is happening in their world in a particular way which serves their ideological interests, that is those of the terrorists. One of the many narratives the extremists apply is that of the Crusades.

Probably I do not have to tell you this, but these were a series of wars, conducted by most of Christian Europe against Muslims in the East in the 9th, 10th and 11th century. The main objective was to capture lands, especially the Holy Land of Jerusalem. And the Crusades also had the effect of serving the political and economic interests of the Europeans. The collective stories of the Crusades form a powerful narrative, as I have described, for Muslims. It includes shared memories of historical defeat at the hands of the West, perceived injustice under foreign occupation and control, perceived economic exploitation and implied religious war. The extremists work tirelessly to link present day actions of western interests, especially the US, to this narrative.

As a part of our research we have conducted, we have collected around 500 texts, public statements and media interviews by Al-Qaeda and related extremists. This graphic shows the average number of occurrences of the word "crusade" in its various forms in the documents of our collection. So as you can see, there are no mentions of crusades, crusaders and so forth in 2000, but then came a steady increase. In 2008 we find an amazing average, amazing to me anyway, of 11 mentions per text. Now it is important to realize that this isn't mere name calling, it is a rhetorical strategy to frame what we in the West were doing in the narrative of the Crusades. The next slide shows these efforts extend not just to the United States but to our allies in NATO.

So for example in 2008 Ayman Al-Zawahiri in his book "Exoneration" said, and I quote, "There is no doubt that we are closely and carefully following the egregious Crusader campaign, which is led by the United States of America with international support from Britain and the Christian countries of Europe, NATO, Russia and the former communist countries." In 2007, Mustafa Abu Al Yazid of Al-Qaeda in Afghanistan said, and I quote, "The strikes of the mujaheddin against the Americans, NATO and the treasonous governments will be a season of victory and conquest for the mujaheddin, and defeat, expulsion and failure of the enemy crusaders and their apostate helpers." In 2009, we saw Abu al-Wadoud of Al-Qaida in the Islamic Maghreb say, quote: "As for the evil alliance led by America militarily and France culturally, and right behind them NATO, the news of our joining in allegiance to you has been like a thorn in their sides and a knock in their stomachs."

I could give you a dozen of examples like this. The question is, why did these messages resonate with the extremists' audience? Well, it is partly because, as Mark said, they are good communicators and they are persuasive. But is also because we assist them with this framing. So you probably are all aware that in 2001 President Bush said, and I quote, "This is a new kind of evil. And the American people are getting to understand this crusade, this war on terrorism is going to take a while, and American people must be patient." You probably also heard that more recently it's been discovered that an American weapons manufacturer has embedded Bible references in the serial numbers of their products. So here we see a gun side with a reference to John 8:12 which says, "I am the light of the world. Whoever follows me will never walk in darkness." So we have Bible quotes inscribed on our weapons. Most disturbing though are these patches that we have found for sale on the internet. As you can see on the top, it says "Pork eating crusader". The same things are written in Arabic underneath, and we have a picture of a guy in a crusader outfit eating a piece of pork. I have first-hand reports that there are active duty military personnel from NATO countries wearing these patches on their uniforms in a Iraq and perhaps in Afghanistan as well.

So these things and more indirect acts from accidentally killing innocent Muslims in military operations to the simple fact of having military forces in Muslim countries for a long period of time is used by the extremists to support the analogy to the crusades. And by the way the crusader narrative is one of many deployed by the extremists. For example they also use the story of the Pharaoh from the Quran to justify actions against Muslim rulers whom they consider apostates. So that is the first point about the role of narratives in strategic communication. It provides an effective way of framing the interpretation of actions in advance for a target audience.

My second point about the role of the narrative relates to something we said about strategic communication in the paper I mentioned earlier. That is, communication and the narratives they contain can take on a kind of inertia. They can become locked in patterns of interpretation that assimilate new messages and resist change. So for example, there are many good reasons why the Crusades are not a good analogy for the actions of the West at present. For example, their being undertaken by secular nations rather than being sanctioned by The Holy Roman Empire which the crusades were, western soldiers are not promised plunder and forgiveness of sins for participating. The objective is not to capture a permanently occupied territory, nor to deny Muslim sovereignty over particular areas. Then we also have the fact that Turkey is a NATO member and certainly, we cannot call them crusaders. Yet no matter how skilfully we make these points, no matter how often we repeat them, we cannot disrupt the Crusader narrative, because it is so well established.

In my mind, this dramatically illustrates the limitations of the old message influence model I described earlier. The narrative is like a balloon. If we press on it in one place, it expands on another place to compensate. And when we let go it snaps back to its original position. So what are the possibilities for dealing with the situation? It seems to me that there are two. The first possibility is to change the existing narrative about us. But because of this property of inertia I have just mentioned, the chances of manipulating or weakening the Crusader narrative by incremental means are just not very good. In such cases, one needs something that will disrupt the existing communication system that will pop the balloon, so to speak. In the US we would call this “a game changer”. With respect to the Crusader narrative one significant disruption would be a break-through in the conflict between Israel and Philistine. This is another narrative that the extremists use by the way, and have been using increasingly in recent years. So a significant change here would go a long way toward disrupting the Crusade narrative. Of course, more is said than done, and I’m not volunteering to work it out but this or some equally dramatic change seems to be the only hope of changing that particular narrative. Given the difficulty of changing the negative about us, there’s the need to consider alternatives.

So a second possibility for changing things is to find a new and favourable narrative to frame the extremists and their actions. A subject matter expert on my grand team has pointed out that the modern day extremists share interesting parallels with the Kharijite, a break-away sect of Islam in the 5th century. They assassinated the last great Khalif Ali ibn Abu Talib while he was at morning's prayers during Ramadan by stabbing him in the head with a poison sword. The Kharijites make a potentially good narrative analogy for modern day extremists for several reasons.

First, the term "kharijite" comes from the "khawarij" meaning those who depart or separate from the group, which these extremists tend to do. It is an outsider term used in the negative sense. Like the extremists, the kharijites believed in the "tekfir", the practice of killing Muslims who are believed to have fallen from their faith. Like the extremists, the kharijites preoccupied with the rigid outward practice of Islam, and like the extremists the kharijits rebelled against Muslim leaders. So portraying extremists as modern day kharijites might be especially effective in Afghanistan, because local tradition holds that Ali is buried in the Blue Mosque in Mazari Sharif and it is a popular pilgrimage site for Afghans. That is one possibility. Another, we just heard yesterday during the presentation by Mr Soofi. He pointed out that Muslims obligated by their religion to honour treaties and treaties signed by Muslim countries forbid the kinds of actions taken by extremists. These two can form an interesting basis for narrative unfavourable to the extremists.

So to summarize, improving strategic communication whereas letting go off this old model that treats communication as influencing people with transmitted messages. A modern approach realizes that communication as a form of dialogue that is heavily influenced by context. Narratives, which are systems of stories, make up a crucial part of that context. Narratives provide a means for people to interpret events and understand what they are doing. Narratives can also assume a kind of inertia making them difficult to change through modest efforts. Accordingly, to deal with the Crusader narrative, we must disrupt it so our communication once again has the possibility to persuade. Another response is to think of negative narrative strategies that can cast extremists in an unfavourable light, making their communication less persuasive.

With that, I thank you for your kind attention, and I invite you to visit our website. The address is shown here that contains white papers we worked on including the one I referenced in the speech. We also have a blog and a thing called "Monitor" which is an aggregation service for other blogs on strategic communication.

Thank you very much.

Dr. Itamara V. LOCHARD (USA)*

"Winning The War Of Ideas: Effective Listening"

Good morning and thank you for your warm welcome back in Turkey. I am delighted to see that this topic on strategic communication has continued since our first fora in it with my distinguished panellists last year in May. In my opinion, strategic communication, as well as strategic listening, has now become the key issue in the department of defence in terms of trying to understand and adapt this new war against terror, war against criminal organisations, insurgents, pirates, militias, gangs.

* Dr. Itamara V. Lochard is the Senior Researcher of the International Security Studies Program at the Fletcher School of Law and Diplomacy at Tufts University. She is also a certified mediator and an Information Operations Expert for the U.S. Department of Defense. Her research explores the nexus of irregular war, governance and non-state armed groups including insurgents, militias, terrorists, complex criminal organizations, organized gangs and malicious cyber actors. She has examined the para-state function of these groups since 1988 most notably at the African Studies Department at the Center for Strategic and International Studies (CSIS), the Institute of International Studies and the North American Forum at Stanford University and the Jebsen Center for Counter-Terrorism Studies. In 2001, she created and continues to maintain a dataset of ~1,700 active non-state armed groups and strategic non-violent action groups larger than 1,000 members. From these data she detects their organizational patterns, areas of cooperation, strategies and tactics. Her current focus relates to their use of Information and Communications Technology in conflict settings, to include Afghanistan and Pakistan. She presents her findings and their policy implications at the U.S. Secretary of Defense Highlands Forum and regularly briefs U.S. combatant commanders as well as senior members of the Pentagon, the White House National Security Staff and National Security Agency. Other notable activities include participating in a ten-member security retreat that drafted a white paper on national security threats for the U.S. President Elect Obama in 2008. She was also a panelist on both the human security and cyber security panels of the Global Creative Leadership Summit sponsored by the United Nations and the Louise Blouin Foundation. In 2009, Dr. Lochard presented on strategic listening at the strategic communication workshop of the NATO Center of Excellence, Defense Against Terrorism in Ankara and lectured on strategic communication and terrorism at a NATO Defense College workshop in Rome. Last year, she also explored presented "Non-State Cyber Threats in BRIC Countries: Brazil" at the Challenges to International Cyber Security conference at the Center for Technology and National Security Policy, at the National Defense University in Washington, D.C. and evaluated of cyber and technology issues for the U.S. Quadrennial Defense Review 2010 at CNAS. In October, she participated in the inaugural EUCOM- Estonian computer network defense familiarization exercise. Dr. Lochard teaches "The Joint-Operating Environment and Armed Groups" to senior-level, U.S. Special Forces at the Joint Special Operations University at Special Operations Command. She has also co-taught a graduate seminar on Internal Conflicts and Wars since 2003 at the Fletcher School; conducted executive training programs to mid- to senior- level political and military officers of the Royal Kingdom of Saudi Arabia, Armenia and the Critical National Infrastructure Authority of United Arab Emirates; and lectured Strategic Non- violent Action seminars. For several years, Dr. Lochard served as a contributing editor to the Journal of Public and International Affairs published by jointly by Princeton University and the Association of Professional Schools of International Affairs. Her academic credentials include a Bachelor in science in Foreign Service from Georgetown University and two Masters degrees from Standford University in International Policy Studies and Latin American Studies. In addition, she holds a Masters in Law and Diplomacy as well as a Ph.D. in International Relations from the Fletcher School. In 2007, she was awarded the Presidential Award for Citizenship and Public Service at Tufts University.

I would like to start with an example of the Titanic. A lot of people think of the Titanic as simply a ship that hit an iceberg and collapsed, and sank. Millions, thousands of lives lost. That actually was not the case. The Titanic is an example of a strategic listening failure. They received six indications that the ship was going to hit an iceberg. They received six separate indications that made it up all the way to the bridge and yet the ship did not turn around. Other ships did. The reason they did not turn around, first, they did not filter the information. They did not pay attention to where it was coming from: from other ships that were encountering similar problems. Secondly, at times the information did not trickle up all the way to the top. And when it did, it was ineffective, because it had been watered down so much. Third, there was a lack of understanding of the real nature of the problem. There were many icebergs where they were, they did not understand the size, and the environment had changed that they would not able to see what they were encountering. We are facing essentially the same situation today, where the environment has changed, the nature of the actors has changed, the amount of vessels in the sea has changed. And the actual sea itself has changed.

What do I mean by this? Terrorism is not new as many people have argued today and as COE-DAT and all of you who focus on terrorism know. There are no new tactics. It goes back to the Peloponnesian War. Neither are criminal organisations or gangs. So why are we still in this? How come they are able to get grandmothers to go online and indicate why they would blow themselves up leaving many people suffering? Even though they do not necessarily lack the finances, it is not a pure economic reason as some have argued. Yet, terrorists are extremely literate in the new media. They are extremely literate in strategic listening to us. They are extremely literate in strategic communications to their populace. They recruit, they retain, they instruct. They coordinate with other groups, non-terrorist groups. And most importantly, they communicate to us, but very few people tend to look at the terrorist videos. I fortunately or unfortunately spent a vast majority of my days looking at them. They are not complicated. They are not fancy. They do not cost a lot to make. They are fairly clear messages to us. Most of them are in English. The English is not perfect. There is always some Arabic in them as well. There is Sufi poetry or Islamic poetry depending on who the target audience is. And you can always see when they are targeting either someone within a particular theatre, whether they are targeting passive supporters to get them to turn a blind eye, whether they are trying to tell us - their adversary - something, to show their strength or to indicate areas of weakness. So there is a lot to be learned by what they are doing in terms of their efficacy in strategic listening. Actually, in Dr. Corman's book, there is an author who analyzed what is called "the brigade of the media jihad", and I think it is an excellent example of how you can see an organisation that spends so much time and energy in information operations, psychological operations, political affairs, public relations. Essentially, everything we do, but the primacy of it is based on listening to us.

Now to understand why the environment has changed, I just want to spend a few minutes on this before going into lessons of strategic listening and how we can implement this at NATO. There has been a dramatic increase in states and people do not fully realize this. If we recall 1648, the treaty of Westphalia that were created to stop all wars against religion.

1648, that is what started the state structure. It took 300 years till about the end of the Second World War to create 50 states. 300 hundred years to create 50 states. From that period of time, from the end of WWII to 9/11, that number quadrupled. And most of those states, as you know, are not completely consolidated. In addition to that, the number of non-state actors who are friendly, international governmental organisations, non-governmental organisations, have increased by fold of 27 times to 300 times depending on which way you look at it. And most of that has happened in the past 20 years, and most of that is in theatre. The third element is that there are 1700 non-state armed groups that are currently active; that are over 1000 in strength, and that are able to create these narratives that Dr. Corman was talking about. I spent a lot of time analyzing them. Not just with statistics, but what are their strategies, what are their tactics, with whom do they work, how do they cooperate, what are the elements of how they evolve and devolve? There is a lot of attention that has been paid in the media and unfortunately it has gained a lot of currency that they are all in weak and failed states. They are there, but there are also a substantive quality, that are also in governed states, in highly governed states. And I have been able to show those matrix. They just take a different tactic, there. They use our governance to use the media, to create their press, to organize .

The other importance is in terms of connectivity. There was a speaker yesterday who talked about cyber issues. What is important here, that I would like to highlight, is that there are about 4 billion cell phones in the world. It is not so much access to computers that allow the jihadists or other groups to access the population. It is through cell phones. Cell phones are disposable, they are hard to trace and when you have that many and they are predominantly in BRIC countries, Brazil, Russia, India, China. Which, three quarters of them, happen to be major cyber states in terms of cyber attacks or botnets, where problems come from. You have a problem. When you also tart looking at the marriages of convenience or the ways that terrorist groups are working with criminal organisations and other organisations, you discover how embedded the issue is, how trans-border, how trans-national.

The good news is that when you are dealing with something that is extremely networked and flat and not hierarchical, often times they do deal with other organisations that are very structured. And if you listen to their communications, if you listen to how they are moving money, it is on their websites, it is in a lot of the blogs, it is in a lot of the videos, it is more easy to trace this type of connection. And it is more easy to then counter it.

We are also in a net speed environment. Information overflow is so dramatic that there is no reaction time. There is information overload. There is a lot of reaction after the event. And after the event, you cannot create your own narrative. We have done a poor job, I would argue, in terms of creating our own narrative in a way that is culturally sensitive to the population at hand. In addition, there is a lot of murky information. Social networking sites, Facebook, Twitter have all been influenced by states, some of them not so friendly as well as non-state armed groups. There has been a decline in professional journalism. There are reports of how the BBC was using tweets and then posting them as real live news. Then they later retracted and started indicating that was their source of their information and they are a very respectable organisation. Again, it points to the murkiness, the fog of war that we are now facing.

Now, a couple of challenges can be demonstrated by a few examples. I know a three star general who is commanding in Iraq, a particular issue in Iraq. He indicated to a group of us that before he went, he spent quite a bit of time reading the Quran, learning about the culture, looking at movies, even trying to learn Arabic. Everything that you would think to do. Once he got there, he indicated he should have been watching the Sopranos or some other type of information to help him understand that actual narrative that was happening at this moment, not just our understanding of what Iraq is or was, but what was currently happening in that particular region. Once he understood the change in environment, he quickly adapted and was able to get tribal elders on board to combat this issue. But it took a while and this is a very respected man. Equally so, as I said, I teach at SOCOM, at Special Operations Command, and we had senior level intelligence personnel indicating what do we do; we have all these bright people who are culturally savvy, who are from the region and yet we can't get the information we need, what is wrong. What we realized is that we are using the wrong paradigm. We are still using a state-centric paradigm. We are not looking at the groups and again this is my mantra because this is most of what I do. And once that has shifted, it has changed now, and it has become more effective.

The UN Office of Drugs and Crime creates some wonderful publications on crime, on drugs, on movement of people and other issues. However, they have zero data on groups. Why? Because there are many states that do not want to indicate problems they have. Equally so, they have a terrorism branch, which is actually quite good, except that it only looks at the legal issues. So therefore, here is an organisation that has so much strength, but does not have the information it needs.

Also, our approach has been to brand, to use a business model, to try to get our narrative across. And that is one of the most ineffective ways to reach any of these audiences. Our approach has been shiny, slick, one to many campaigns, assuming that we have one audience. And that does not work. Posting a reaction to whitehouse.gov or on a blog of any type of organisation is not enough. It is a start but it is not enough.

So what can be done to deal with the classification levels, the difficulties with trickling information up, the difficulties of having text-savvy people at the front line who understand the technology that is happening, who understand what is being done, but don't have the ability to provide the information in its full strength to the commanders. What can be done to deal with the high turnover where you cannot keep lessons learnt?

Few suggestions in my last few minutes. Number one: understand the audience better. That includes adjusting your assumptions. This was done by the Holbrooke Secretary Clinton's envoy to Afghanistan last year.

Basically, it was an attempt to ask the simple question why do you think that the terrorists are here? What is their appeal? They wanted to hear it from the people, from the tribal elders. So that we are no longer just looking at our myopic view, and it has become very successful even though it sounds simplistic. Another thing is to look at language. For example, the Eskimos have 150 words for snow, in English we have one. It demonstrates when you look at the language how important a particular issue or topic is. Therefore, you can talk about whether you should be using terms like democracy or honour. Another issue is to be open to the new media that is out there: the social networking, the blogging, not just news reports. Because they are no longer the true source or voice of what is happening; taxonomies, something as simple as increasing your situational awareness from the frontlines. When they go into an area, some people have indicated to me some special operations officers, that they go and they actually look what is in the supermarket, what is not, what can they see. Again, this sounds like basics, increasing your situational awareness. But that is truly what is required.

Another element is high to low context cultures. Our culture tends to be low context. We are not as interested in the environment; we are interested in the fact. When I say our, I mean the West. That is not the case for most of the Asian cultures. That is not the case for most South-Asian cultures. Similarly issues having to do with the way people deal with body language. How close they stand to you? Whether they look at you in the eye, whether they use this to mean stop or not. Whether shaking your head side to side means actually yes. Simple things like that have caused a lot of complications, a lot of friendly-fire issues, a lot of misunderstandings, a lot of inability to communicate effectively and inability to listen effectively and a long time in getting proper interrogation procedures.

Cultural views on deception is something else to keep in mind. Some people would argue “A lie is a lie is a lie". However, in certain cultures deception is actually seen for the greater good if it creates more harmony. In some cases, it can be very mild, in other cases it can be more excessive. But without having that cultural landscape, you miss what the person you are speaking to is actually about. There is a lot of focus on Afghanistan and prior to this, on Iraq for good reason. However, terrorism is not only there, and these groups are everywhere.

A third thing would be translation versus interpretation. A lot of the issues have been about not just simply interpreting the words into a language that we can understand, but into a problem that has occurred, has been there. People have been actually translating or putting their own bias into it. That has caused a lot of problems, because there hasn’t been enough cultural sensitivity in the training. Because the rotations have been too quick.

Last: fragmegration. This is a term by Rosenau and what he argues is that you have two competing forces that happen in most of these areas. You have the global have-nots, those who are not the tech-savvy, who don't have the cell phones, who don't have the computers. They feel de-segregated. Then you have those who are the "haves", so to speak. So those who do not have, tend to become more insular, go back to the things that they understand: their basic narratives, their basic explanation for why there are in the problems that they currently exist. By looking at that analogy, you can see who are the people who control the communications in a particular theatre, who are the ethnicities or which ethnicities are actually savvy to that technology, which one has access to it by religion, by gender, by ethnicity. By doing so, you can see which ones are allying with whom. It has been a very effective thing to look at.

Finally, I would argue, look at the precipitants versus preconditions. What is the cause of the conflict, not just the spark? The assassination of Archeduke Ferdinand is not what caused the World War, we know this. However, because of our lack of understanding of the adversary, we tend often to confuse precipitant versus preconditions. And if you are addressing the wrong issue, you cannot get to the root problem.

Winston Churchill argued great leaders are great listeners. They are engaged, they ask about the landscape, they understand narrative. I argue we should do the same thing today.

Thank you.

THIS PAGE IS INTENTIONALLY LEFT BLANK

KEYNOTE ADDRESS

Mr. Guy B. ROBERTS
Deputy Assistant Secretary
General for WMD Policy, NATO

THIS PAGE IS INTENTIONALLY LEFT BLANK

Mr. Guy B. ROBERTS (USA)*

"The Threat Posed By Biological Terrorism"

Well, thank you very much. It is a great pleasure to be here and so wonderful to have this opportunity.

Admirals, Generals, Colonels,

Distinguished Guests,

Ladies and Gentlemen,

It is a pleasure to be here once again. I have been here, giving presentations at the Centre of Excellence Defence Against Terrorism a couple times in the past. And it is always gratifying to know that I did well enough to be invited back.

I am going to speak to you today about the threat posed by biological terrorism. You have heard Prof. Allison speak yesterday about the threat of nuclear terrorism, and it is only fitting then to address the issue of biological terrorism in an appropriate talk also; I wanted to emphasize this.

* Guy B. Roberts is the Deputy Assistant Secretary General for Weapons of Mass Destruction Policy and Director, Nuclear Policy Planning Directorate for the North Atlantic Treaty Organization (NATO). In that capacity he is responsible for developing policy on issues related to combating the proliferation of weapons of mass destruction and overseeing NATO's nuclear deterrence posture. Previously Mr. Roberts was Principal Director for Negotiations Policy in the Office of the Secretary of Defense responsible for advising senior Defense Department officials on the entire range of United States arms control and non-proliferation policies. He was also responsible for implementing policy guidance and DoD positions for current and emerging proliferation issues in mulitlateral arms control and disarmament fora. From 2000 to 2003, Mr. Roberts served as the legal counsel for arms control and non-proliferation in the US Department of the Navy. He was responsible for reviewing all naval programs to ensure compliance with all arms control and nonproliferation agreements and developing policy on all arms control and nonproliferation agreements or initiatives, which could impact Departmental equities. Prior to that Mr. Roberts had a distinguished career in the US Marine Corps before retiring, holding a wide range of assignments in policy formulation, operations support, negotiations, management, litigation and policy/legal advisor both in the US and during overseas assignments. Positions and responsibilities included legal counsel to a four-star Combatant Commander, and military representative for disarmament and arms control issues to the United Nations, Conference on Disarmament and the International Atomic Energy Agency. Mr. Roberts received his law degree from the University of Denver, and he holds masters degrees in international and comparative law from Georgetown University, in international relations from the University of Southern California, and in strategic studies from the Naval War College where he graduated with highest distinction and won the Stephen B. Luce Award for academic achievement. He is admitted to practice in Colorado, California, Arizona and before the Military Court of Criminal Appeals and the US Supreme Court. Mr. Roberts has written extensively on nonproliferation, arms control, terrorism and law of war issues.

What I call the most horrible of horrible events is the threat of biological terrorism. I want to begin by providing you a brief overview of bioterrorism and the role that science plays. I do want to explain to you the nature of the current threat before turning to the evolution of NATO's policy regarding proliferation issues with a focus on the bioterrorism threat. I have to admit right up front that this is a very challenging and most difficult area for the Alliance as it is for our nations. Frankly, our record on this is somewhat mixed.

Since I am the first speaker after lunch and it is always the most difficult time in order to kick things off, I would like to begin with a story, which, I think, relates very well to the problems we have in dealing with bioterrorism. It is a story of two American hunters. They go up to Alaska to hunt for bear. So they fly up to Alaska, they land on this lake. The pilot says, “Well, I just want to tell you, you can only bring back one bear.” So three days later the pilot flies back, lands and there is the two hunters with two bears. And the pilot says, “Well, I told you, you can only fly back with one bear.” And the hunter said, “Well, look we will give you a thousand dollars if you will take both of us and the two bears." And the pilot thinks about it for a minute, and says "Ok!" So they load the two bears on the plane, two hunters get into plane. The plane takes off, goes about ten kilometres and crashes. Miracle of miracles the two hunters survive and one hunter staggers out of the plane, he looks around and he says, “Where are we?” And the other hunter looks around and says, “Well, I think we are about five kilometres farther then we got last year”.

That is kind of how we are dealing with bioterrorism. We take off, we crash and then we keep on going. I do want to discuss with you, some of those activities though, and I do have a story to tell and we are doing a lot; we could be doing a lot more though. This is a very challenging and difficult area mainly because it is of such a remote nature in certain respects that our politicians, the ones who control the purse strings are willing to provide the resources necessary to actually, effectively deal with what is a real threat. Obviously I do not have to remind this audience about the gravity of terrorism. Terrorism is certainly a feature of daily life, in almost every corner of the world. Terrorist acts routinely take hundreds of lives and often dominate the daily news. These events of course, though, pale in comparison to the devastation of a terrorist attack with biological weapons. Bioterrorism represents certainly a challenge to the international society. It is not a new challenge by any means neither is nuclear terrorism. But it is a significant and potentially far devastating challenge than anything else including, in my view, a nuclear attack. Major biological weapon attacks on one of the world's major cities could cause as many, if not more, deaths and as much, if not more, economic and psychological damage as a nuclear attack.

In that regard I disagree with Prof. Allison. Given the widespread access to the relatively unregulated technology, to materials, agents, and know-how, I believe it is far more likely that we will see a bio-attack than that we will see in fact a nuclear attack. I have also to admit there are lots of predictions. The WMD Commission in the United States and others predict that there might be an attack with either a biologic or nuclear weapon in the next, I guess, five years from now. But I certainly do not want to engage in that. For me it is very difficult to predict these things. If I could predict the future, my stock portfolio would not look as bad as it does.

But nevertheless, it is, I think, a virtual certainty that we will have future epidemics and pandemics whether naturally or even potentially deliberately caused. And it is hard to say when; but it is certainly, I think, obvious that these things are going to happen and we need to be ready for it, we need to be prepared. There are certain things we can do, and there is certainly no secret to the fact that if terrorists should ever acquire these weapons, acquire this capability, they will use it. They are not going to acquire either a biological weapon or a nuclear weapon for deterrence purposes. They are going to use them in a way that a terrorist would in order to again cause severe economic and psychological harm to our societies.

NATO recognizes of course that WMD terrorism comprises the possibility of attacks from a variety of substances: chemical, nuclear, biological. In fact we had the Tokyo sarin gas attacks in 1995, the death of Alexander Litvinenkow with Polonium 210, and recently the gas attacks in Iraq, obviously perpetrated using these kinds of substances.

I will focus today primarily on the bio aspect. As I said, while nuclear weapons would cause maybe the most devastating attack in terms of the shier impact, biological weapons are more difficult to counter. As we noted in the WMD Commission report, the United States and other countries, or in fact, I would even say all NATO countries, would receive a failing grade in terms of developing the capabilities to counter this threat and having plans in place for recovery. What I do want to do though, I want to illustrate some of the work that NATO is doing in this field. And as I said before we have some good stories to tell but a lot more work that needs to be done in the future.

First of all, let me explain what I mean by bioterrorism. There are many definitions, this one I like to use is the one provided by Interpol: “the threat from bioterrorism poses many challenges for not only national authorities but the international community as a whole”. One thing, I would add to this, is, that the impact of this form of terror would be most likely multinational border crossings. In order to deal effectively, it would require coordinated communication, coordinated response, and of course investigative efforts to determine whether this was in fact a deliberately caused or naturally occurring event.

Biological agents are categorized briefly depending on their potency, ease of transmission and probability of being weaponized. Category A is the most lethal and the most concerning category for the prevention of bioterrorism. We are especially concerned with category A agents for several reasons. The agents can be easily disseminated or transmitted from person to person, results in high mortality rates and have the potential for major public health impact. It might and will cause public panic and social disruption and will require special action for public health preparedness.

Around the world we are in fact experiencing an unparalleled period of scientific advancements and innovation in biology. Biotechnology in my view is the business of the 21st century. There are thousands of biotech firms springing up all over the world, and they are developing a number of new agents and treatments for all kinds of diseases and all kinds of new capabilities in this area. Techniques that were once cutting edge innovations now are becoming more and more commonplace. Capabilities once found only in a few advanced laboratories are now increasingly widespread throughout the world, and continually pushed down.

Today in high schools around the world, young students are doing experiments that 20 years ago may have earned them a Noble Prize in biology. To compound matters, in addition to traditional bio threats, potentially a new generation of bio weapons have begun to emerge.

The revolution in modern genomics has allowed for rapid advances in the ability to modify and manipulate genes in bacteria and viruses, and these processes can be used for good and they can be used for evil. In recent years we have also seen scientists creating synthetic pathogens. These pathogens can be modified for different purposes. For instance, the Centre for Disease Control in Georgia has recreated the 1918 influenza strain. Now this was a flu strain pandemic that killed 25 to 50 million people. They have modified this particular strain to make it thousands of time more deadly. In addition to recreated pathogens we have seen once, they have created pathogens that have no prior history in the natural world. Of course we have the perpetually mutating influence of virus that again every year kill hundreds of thousands of people. We have also seen increasing experimentation using nanotechnology, like synthetically created organisms. Nanotechnology does have legitimate uses that Prof. Özbay discussed earlier today. And they have potentially revolutionized the medical field by making traditional surgeries, cancer therapies, vaccines, things of the past.

However, continuing or combining biological components with programmable technologies also poses risks that can be exploited by those bent on causing harm. There has been research already done on programmable nano particles that can make someone have a heart attack or cause brain haemorrhage or disrupt regular body processes. Of course this is a no-secret to this group; but as I said earlier, terrorists groups have been very much looking at ways how to acquire the capability to use weapons of mass destruction in general but also, and particularly, biological weapons. Al-Qaeda of course is the one actor of greatest concern. It has the funding and logistical means to carry out such attacks. It has the greatest desire and means to acquire biological weapons and it has made it clear, very clear that it will target NATO and other allies with these weapons.

Recently, Ahmad Salma Mabruk, member of the Egyptian Islamic Jihad, claimed that Al-Qaeda possesses chemical and biological weapons. We have no evidence of that but he made this claim. Another Al-Qaeda operative, Abdullah al-Nafisi, has tried to recruit white supremacy groups in the United States to aid in the spread of anthrax around the US. More worrying still is the call by Abu Ayyub Al Masri in Iraq for scientist to join the Jihad because Jihad could satisfy their scientific ambitions, and the large American bases in Iraq were good places to test unconventional weapons whether biological or dirty nuclear devices. Obviously these weapons, if they acquire them, they will use them; they are not going to be used as a deterrent.

I mentioned the attacks in Tokyo by a nihilist group, Aum Shinrikyo. This group was one of the first, not "the first", but one of the first to attempt to weaponize biological agents for use against citizens before the successful sarin gas attacks which killed over 13 people, and in which over 6200 people got sick. In 1995 this group actually dispersed anthrax spores that were thrown off a building into a large group of people below. The only thing that prevented casualties was that they did not aerolise the spores properly, so they were not infectious. Also you may remember the anthrax letter case in the US in 2001. This attack led to the infection of 22 people and the death of five. Despite the small quantity of dry spores used in 2001, the event caused massive panic, shut down US government, had a significant impact on transportation, schools and people going to work, and by one estimate cost up to 6 billion dollars in lost economic productivity. So in this case, I would categorize this weapon as not only a potential weapon of mass destruction, but a weapon of mass disruption. Certainly, terrorists have taken note of this, and obviously continue to look and seek for ways to obtain and use it. We certainly have enough information and intelligence to indicate that they are continuing to try to acquire this capability.

NATO of course recognized the danger of WMD terrorism generally and the bio threat more specifically. It was only after 9/11 2001, however, that we launched specific initiatives to address the threat of bioterrorism. Generally, we say that in WMD terrorism, WMD proliferation is the primary threat and will be the primary threat to the Alliance for the next 15 years. So in order to address this threat, in 2001 we created the WMD Centre at NATO headquarters to improve intelligence and information sharing about proliferation issues and not only on chemical biological, radiological, nuclear weapons but also ballistic missiles. At the 2006 Riga Summit, NATO governments agreed on a document "The Comprehensive Political Guidance." This document recognizes terrorism and the spread of WMD as the principle threats to the Alliance.

At our 60th anniversary summit last year, our head of state or government endorsed a comprehensive strategic level policy for preventing the proliferation of weapons of mass destruction. This is the copy. It is downloadable on our website; this document is a political mandate to, in fact, develop a number of initiatives to address the proliferation threat and the WMD terrorism threat.

Now, I would like to also discuss briefly the initiatives that NATO has undertaken to specifically counter bio threats. This is an illustration of some of the guidance and tasks we have been given by heads of state or government in the last couple of years. The link between terrorism and WMD was spelled out at NATO's 2002 Prague summit. Allies there committed themselves to improve and develop new CBRN Defence capabilities and to enhance NATO's role in the fight against terrorism. At the Prague Summit, we had a package of key military transformation measures agreed to enhance the Alliance's military operational capabilities including these five initiatives you see here.

Some of these I have already discussed, some I will not. For example, the virtual pharmaceutical stockpile, and this is virtual. I will not discuss it, because we could not get any nation to agree, to provide virtual vaccines. So this has been a challenge again, because there is a cause factor involved but also a political factor about releasing vaccines in the case of a crisis in which you would not be able to provide them to your own population, if you provided them to NATO. In order to reduce the possibility of biological attacks, several initiatives have been developed that focus on prevention and protection. These initiatives are multi-faceted. They emphasize information sharing which is a critical aspect of being able to develop the capabilities to respond to any potential threats in this area; interstate cooperation and developing actionable intelligence to strengthen our non-proliferation initiatives. NATO is working towards increasing cooperation and coordination with friendly nations, partner nations as well as international organizations. These efforts allow us to exchange information with nations and other international governmental organizations regularly on biological threats that may be developing regionally. This network of partners extends to the Mediterranean area to reflect NATO's view that security in Europe is tied to the security and stability in the Mediterranean. Similarly, the Istanbul Cooperation Initiative is also meant to promote practical cooperation on a bilateral basis with countries in the broader Middle East. And again we are looking for ways in which we can partner with these countries to help develop mutual capabilities to respond to these kind of threats.

In order to increase the collaboration with other international governmental and non-governmental organizations, it is also important to be an active participant, and organise conferences such as this and other workshops. Last September we participated in just such a conference in Switzerland, 35 NGOs came together to discuss illicit trafficking. During that discussion, we were asked to brief on each one of our capabilities. And it was quite amazing to hear what many of these organizations have in the way of capabilities in order to avoid duplication, in order to achieve what we call the comprehensive approach within the Alliance. It will be increasingly important that we do partner with these organizations, and critically start sharing information about our mutual concerns dealing with the full panoply of illicit trafficking.

To enhance coordination among Alliance members, NATO has established the Terrorist Threat Intelligence Unit (TTIU) at headquarters in 2003. This unit draws on civilian and military intelligence resources from both NATO and partner countries in order to provide assessment to the North Atlantic Council. The TTIU works on terrorist threat analyses and provides threat-related information to NATO decision makers. At the Istanbul Summit in 2004, NATO country heads of state and government agreed to review intelligence structures and mechanisms and endorsed a programme of work for defence against terrorism. This programme aims to equip NATO's armed forces with new or adapted technologies to detect, disrupt and defeat terrorists. It also focuses on providing rapid response capabilities for the protection of civilian populations and infrastructure, particularly in the area of WMD. I cannot emphasize enough the importance of intelligence in this area, and this is one of the primary functions that we have with the WMD Centre working in partnership with the Terrorism Threat Intelligence Unit.

The partnership action plan against terrorism is also a framework which allies partner countries as well as organizations such as the EU, OECD and the UN to improve cooperation in the fight against terrorism. The action plan facilitates greater intelligence sharing and cooperation in areas such as border security, terrorism-related training and exercises, the development of capabilities for defence against terrorist attack and for managing the consequences of such an attack, again in this case with a focus on WMD.

As I said I am not going to mention all of the centres of the initiatives but the one that I do want to mention, because I believe it is the critical one, is the disease surveillance and analysis centre that was recently set up in Munich, Germany. This centre achieved interoperability in June 2007. They were planning to have the capability to come online, and in the 2010 to 2012 timeframe it will provide a continues threat assessment on field outbreaks of diseases and send immediate feedback to operational areas and the NATO command structures. Assessments rely on available public health statistics on disease transmission and prevalence which in turn involve intense cooperation with public health data bases and alert systems.

Now, this is a very critical capability, and in order to demonstrate that capability I would like to show you a couple of videos demonstrating what could happen in the event of a biological attack without the bio-surveillance network and with it in place.

VIDEOS STREAMING

Ok! Well, you can obviously see why I make such a big deal about our disease surveillance network that we were setting up in Munich. It will make a fundamental difference if we have this capability, and it will have an impact on military operations.

Let me briefly talk about a couple of other things. One is the Centres of Excellence. Again this Centre for the Defence against Terrorism is one of our key partners and an important education and training centre to help talk about these issues. This centre of course has a programme that includes bioterrorism; I ran a bioterrorism workshop last year, and I know they will continue to do that. We also have a Centre of Excellence in the Czech Republic. The Czech centre also provides training, does research, knowledge exchange and capacity building in the area of CBRN. It provides advice on all CBRN defence-related issues, it develops CBRN defence doctrine standards, knowledge of support, improvement of interoperability, and capabilities. Also, there is a centre there for bio defence which includes a specialized infections hospital for people infected with dangerous and exotic agents of bio safety level 3 and 4 conditions. This is about a 50-bed hospital and it is the only hospital of its kind in the world. It does not exist anywhere else. I believe the WHO has a 10-bed hospital in Rome. When we had that conference back in Switzerland last September, when we briefed the WHO on this they were surprised, had no idea that NATO had this capability and now we are engaged very actively in a programme to try to work with WHO who may want to use this facility for training and for potential exercises with NATO. This is one example again of building these habits of cooperation with other international agencies.

Should a terrorist group or a hostile nation succeed in launching a bio-attack, again we have put together some tools to try to assist nations. The Euro-Atlantic Disease Response Coordination Centre was established in 1998 with the objective of coordinating the provision of mutual assistance among EAPC Euro-Atlantic Partnership Committee countries and Mediterranean Dialogue countries. Originally, it was intended to respond only to natural and technological disasters but during conflicts it also provided humanitarian assistance. And in 2001 the North Atlantic Council gave a CBRN mandate. The inventory of national capabilities, which is included in this, is a list of capabilities that would be required for immediate response needs in case of a CBRN attack against our civilian population.

The Civil Emergency Planning Crisis Management also advises various NATO bodies and monitors developments following an attack with the help of civilian experts. NATO has about 360 civil experts that can be deployed if needed out in the field to assist our rapid reaction teams in an emergency. We have also created a multi-national CBRN defence taskforce. It is relatively new, but it reached operational capability, and in late 2003 we have deployed it to several civilian activities including the 2004 – 2006 Olympic Games. It provides NATO with the ability, a limited ability, to respond and manage the consequences of WMD use both in and outside NATO's area of responsibility.

NATO cannot hope of course to counter terrorism on its own, and as I hinted at earlier on, we are working on partnerships with a number of different organizations. Just let me mention a couple. I already mentioned the World Health Organization; the EU is also an important partner in their fight against terrorism; recently a strategy against the proliferation of weapons of mass destruction has been established. And our contacts are increasing with the two organizations. In fact, next week I will be meeting with my counterparts to discuss bio-threats and cooperation in dealing with bioterrorism and what capabilities we have in the area of bio-preparedness. As with Interpol, of course, as you may or may not be aware, Interpol has the task to further coordinate, develop and enhance knowledge, training, and capability of law enforcement agencies in dealing with WMD threats. They have also established a bio-forensics laboratory, which we are interested very much in partnering with, to use that capability. Again if we can use Interpol's capability then that capability, we, NATO do not have to develop it on our own. But as I said before we are looking at reaching out to other organizations, these are just two examples. We are also developing a relationship with the European Centre for Disease Control and the US Centre in Atlanta.

Let me just close by mentioning a couple of other things that we are doing; we have a rapidly deployable Outbreak Investigation Team capability. This is a national contribution; at least seven nations have contributed to this capability. These teams are deployable within 48 hours and they have identification mechanisms on what agent might be used, they can carry out epidemiological investigations and perform sampling for lab forensics. And they can also advise on the prevention and control measures to be taken to limit outbreaks. The Alliance is also currently in the planning phases of developing a non-proliferation trust fund that would primarily support the goals of the UN Security Council Resolution 1540 and the non-proliferation activities of the Alliance. These projects would include the creation of regional non-proliferation centres and the deployment of mobile training teams to assist nations in complying with this UN Security Council resolution.

We have also been looking into developing programmes that help countries develop their capabilities to fight the fire against bioterrorism. For example, we recently helped set up in Romania a bioterrorism and bio-preparedness centre which is a combination of governmental agencies and non-governmental organisations.

I have basically gone way beyond my time and I do not have anybody telling me to stop. So, I will just wrap it up here. Again I think the key message that I would like to make with this presentation is that bioterrorism is something that we definitely see as a potential threat, that we are developing capabilities against this threat, one example being the Munich Centre I mentioned. Nevertheless, we have a lot of work left to do. We would like very much to reach out to partners, reach out to countries that would like to partner with the Alliance to help work on developing these capabilities to stop this threat. As I said, we are at the very beginning. This threat knows no borders. In order to effectively deal with it we are going to have to work together. We are going to have to develop mutual capabilities to mutually reinforce our responses, and only through full cooperation will we have any real hope of being able to stop what I call the most horrible of horribles.

Well, thank you very much, it is a pleasure to be here, and I look forward to our discussion about this at a later time. Thank you!

FOURTH SESSION
QUESTIONS AND ANSWERS

Q: Ahmer Bilal SOOFI: Thank you very much. It was extremely useful to hear the panellists. My name is Ahmer Bilal Soofi. I wish to bring the attention of the panellists to the issue of communication skills that the terrorists have. What we are talking about here is how they communicate their message to the media. My concern is how they communicate the message to people around them in the villages as well, in the communities and the message they communicate to gather more sympathisers. They specialize the skill of public speaking which is developed methodically and extremely systematically. They are taught debating logic; they are taught specialized skills of how to handle questions and answers. And they are taught how even to be cursory and sketchy without substance and yet be convincing in the eyes of the media and in front of people. This is a very specialized area that in my understanding has not been properly understood. In response to their oversimplified logic which appeals to the public, we, while sitting here, from NATO HQs, or from Washington DC or from London respond in a very sophisticated manner. That sophistication is no match to the logic and debating skills that they possess. An example I can give you is, if you have a debate in the media between a religious scholar and a liberal, you will find that he is totally outsmarted by virtue of the skill which they command. This skill is evident from various speeches which they make. So I think there is a need to understand that skill, there is a need to match that skill by either training people who can develop similar skills and match them. Otherwise the sophistication of the response will not be a sufficient answer to the logic, to the debating skills they possess.

A: Dr. Itamara LOCHARD: Thank you very much. I actually very much appreciate your comments yesterday when you presented your talk because it added a new element of how to deal with this. I would argue a few things. I agree with you entirely. But some examples we didn’t have the time to go into all of it. I know they have been working on it in the US. They have been to looking at and highlighting what the areas are where the radical Islamists are making mistakes, where it doesn’t match the Quran. And you provided an excellent example yesterday. And highlighting those, we do not do enough to show their mistakes whereas every single mistake we make is amplified.

Similarly a lot of people who talk about narrative, I will leave that point to Dr. Corman, argue pretty strongly that you shouldn't try to counter it. Because then you are always on the defensive. It is better to just constantly put out your message in a clear way to those people, which is precisely why I was talking about the cell phones. If you put your answer on a website and people are just receiving text messages, it is disconnected. There are ways to counter that. Last thing I'll say is there is something called insider-partiality which is a conflict resolution term that was used for the mediation by the United Nations. Basically, it is using local people who are partial because they are local, they have to live in the environment, but who are insiders and can help provide the understanding of the people. Because there is no way, no matter how well you try to understand a culture, that you can grasp what is happening on the ground. Thank you.

A: Mr. Mark LAITY: It is an interesting question on the skill of communication. I am unaware that the Taleban or other insurgence groups kind of run speaker's schools. I would be interested if they are. I think what they do have; they have certain natural advantages which are, let's be blunt. They are of the society to which they are speaking. That gives them a natural advantage. No westerner, no matter how articulate, how skilled can have that kind of empathetic feel which will often serve somebody who was otherwise less articulate. So I think they have a certain natural advantage and they generally do come from the society to which they are speaking. So they have the finger on the pulse. That is the advantage they have. I think there is also one shouldn't overplay them.

When they have done analysis of, and there have been recent analysis, communications, and I speak particularly of Afghanistan where there is a mixture of terrorism and insurgency, most, the majority or a significant majority of the communications they put out is intimidation. The prime message which comes from insurgents and terrorists is "you do it or else". So they are not that sophisticated. Another point is that the Islamic tradition of rhetoric is something we find, and non-Islamics find, very hard to manage. We have to learn that rhetorical way of speaking which in many respects comes very naturally to people who come from that community. Because you are brought up with the Quran, just as I'm brought up with the Bible. Now, beyond the beliefs which overlap hugely as we know, there is a style to the Bible, and a style to the Quran which bleeds into public life, into discourse. That is where we have a significant problem. Then finally on sophistication. One point I didn't make and perhaps should have one of the things we need to learn is simplicity versus complexity. Keep things simple. A few statements, a few messages, few key points constantly repeated succeed far better than overly sophisticated messages. That is one of the faults we have. It is because we are complicated organisations and end up with complicated messages. That is neither necessary nor effective.

A: Prof. Dr. Steven R. CORMAN: Thank you for the question. I was very interested to hear you say that one of the tactics that the extremists use is to be cursory and sketchy in the things that they say. This is not to promote our papers anymore than necessary but we have another paper on the website entitled "Strategic Ambiguity and Strategic Communication". The idea of strategic ambiguity is that you try not to be too explicit in the messages you put out because in doing that, you allow the audiences to participate in the construction of the points that you are trying to make. This is something I think we failed to grasp in the West and it goes well along with this old message influence model that I send messages to you and it sort of hits you in the head and persuades you. It is a control-based model that Mark rightly said, we have to let go off. So, more practice of that sort of thing along with the point about being simpler in communications is a good point.

Finally, I think what you are saying basically is that in many cases, because of the asymmetries involved here and so forth, we cannot be the ones to deliver these messages and after all, we are the Crusaders, right? So we do not have the credibility to deliver, for example, these new narratives comparing the extremists with the Kharijits and so forth. We have to rely on people from the culture to do that or persuade friends in those cultures to do that.

Q: Lieutenant General Masood ASLAM: Pardon me for my bad throat. I am Lieutenant General Masood Aslam from Pakistan. I want, first of all, appreciate and comment on the subject which was presented today. Because there is no doubt that today strategic communication is actually the foremost tool which anybody has today to counter insurgency as well as terrorism in the world. The point which I want to raise is two-fold. As General Petrus has said, in all counter insurgency operations, the foremost thing which all military planners understand is the terrain. And the terrain in this case is the people. So that means it automatically signifies the importance of reaching out to the people. So that means, it is the social space which the terrorists or the insurgents are trying to occupy, and that, the social space, is what we are trying to deny to the terrorists. The aim, the fight is actually to contest that social space which allows terrorists to exist in a particular society. That means that when we are planning an info or psychological campaign, we need to be mindful of target audiences. And the narratives for each target audience have got to be different. These are target audiences of the locals from where the terrorists actually draw support, maybe passive or active. Then there is a target audience of the people in general in that country, it may be Pakistan, Afghanistan or Iraq; and then the third group is the Muslim world as a whole.

And finally, the target audience is the West because the West has got to be kept motivated to continue to support this effort against insurgency in that region. Therefore, you can understand the significance of all types of narratives which we have to create. The symposium, the global cooperation for counter insurgency actually is the right thing, how each society, how each nation has got to cooperate for undertaking various narratives. These are some of my observations.

One more point I would like to highlight which Vice President Joe Bidden who, before he took office in January last year, visited Pakistan. In one of the meetings after that, when we were discussing about the local sensitivities and the effects it had while framing strategies for an area, he made a mention of his childhood. He said that, when we were young kids, on weekends we all would like to get a night out or some money from our mother. To be good kids, we would like to be very helpful to our mother and jump into the kitchen and ask her to let us help and do the job. And our mother used to tell us that we sit down, “if you want to help me, help me my way. But I am finishing here “that help me my way.” So, let’s not try to do it our way to the people in that particular region. Thank you sir.

Comment: Prof. Dr. Steven R. CORMAN: That is a very good point. The terrain is here basically the social terrain. This is one of the reasons that we think this new communication model is needed where communication is viewed as dialogue, rather than just sending messages out to people. Because, only through dialogue you can really understand people’s perspective and adapt to those and take them into account. I agree with that completely. I am a little concerned about the idea of having different narratives for different audiences though, unless you are extremely careful in doing that.

Because the problem is that you might have a narrative for one audience that contradicts the narrative for another audience and then that damages your credibility. So that is something we have to be very careful about doing. As Itamara said, in the age of the internet you can't tightly target the audiences anymore than the way you used to with messages. Because they tend to leak out all over the place. The point you are making is a good one, that you have to adapt to your audiences, at the same time you have to be careful about doing that in a way where your messages or narratives do not contradict one another and damage your incredibility.

Comment: Mr. Mark LAITY: I would like to loudly echo what Steve said because it is an important point that the key to any narrative is that it must be consistent across anyone who is likely to hear it. Because credibility has always been a principle factor of information and that does not change. Certain things do not change. Speed is one, credibility is another. So if you have differing narratives which can contradict, then you have a form of fracture-side. So what you need to, and that is one of the reasons, it is somewhat easier for the terrorists or insurgents, is that very often their narrative is simpler and has easier central cores. For instance, I would contend that at every level of the narrative of the terrorists or particularly say the Afghan insurgence, there is a core fear. Obviously, they are trying to scare the West and then with the Islamic communities which they are appealing to, they are also threatening them. It is a dual approach. So there is a core of fear. At whatever level, the terrorists' narrative is looked at; it has its core fear. I am actually acting in their interest but frankly if you do not go along with it I'll kill you, or if you are dealing with the West, you Crusaders, you better back off. Our narrative is much more complex. It still needs to be consistent but we need to have a central core narrative and indeed there will be NATO launching a project to try to deal with this very issue of a narrative that we resonate both with Afghans and with contributing nations. It can be done but it is a very, very hard task. But if you have differing narratives, you would definitely lose.

Comment: Dr. Itamara LOCHARD: Thank you for your comments. I would agree with what my panellist said however I would also agree with you in the sense that where terrorists have been particularly effective has been in recognizing that there are so many audiences. They do not provide many different narratives, but they just recognize there are so many audiences that need to be confronted, that need to be appealed, and that need to be spoken to. Whereas I think where we have failed in the West is to recognize how many actors are actually involved, that you need to look at, the passive side, that you need to look at the external support and that's one part where I think we can improve quite a bit. But I agree entirely that you have to convey your message as clearly as possible. Thank you very much.

FIFTH SESSION

THE ROLE OF INTELLIGENCE IN COUNTERING TERRORISM

Chairman:

Prof. Dr. Ali L. KARAOSMANOĞLU
Bilkent University

Speakers:

Prof. Dr. Antony H. CORDESMAN
Centre for Strategic and
International Studies

Assoc. Prof. Wesley K. WARK
University of Toronto

THIS PAGE IS INTENTIONALLY LEFT BLANK

Prof. Dr. Anthony H. CORDESMAN (USA)*

"Military Intelligence In Countering Terrorism"

Good afternoon ladies and gentlemen. Thank you for the opportunity to talk about the subject this afternoon.

Military intelligence in countering terrorism is an extraordinarily complicated subject, and working with a number of countries and with an Alliance context in the past, I am also struck by how different the needs of given countries can be depending on the nature of the threat and also on the nature of their neighbours, and depending on how they structure their efforts. But I think there are some clear messages that can be given. In that we have learnt, and learnt over a very long period of time.

First, there is a real danger in the phrase "military intelligence". The fact is that particularly when we are dealing with asymmetric warfare terrorism and insurgency, military intelligence is not the approach any country should use to the problem of intelligence or any military should use in the approach to intelligence. We need what we call "fusion", we need to understand that the military have to

* Anthony H. Cordesman holds the Arleigh A. Burke Chair in Strategy at CSIS. He is also a national security analyst for ABC News. His analysis has been featured prominently during the Gulf War, Desert Fox, the conflict in Kosovo, the fighting in Afghanistan, and the Iraq War. During his time at CSIS, he has been director of the Gulf Net Assessment Project and the Gulf in Transition Study and principle investigator of the Homeland Defense Project. He also directed the Middle East Net Assessment Project and was codirector of the Strategic Energy Initiative. He has led studies on the Iraq War, Afghan conflict, armed nation building and counterinsurgency, national missile defense, asymmetric warfare and weapons of mass destruction, global energy supply, and critical infrastructure protection. He is the author of a wide range of reports on U.S. security policy, energy policy, and Middle East policy, which can be downloaded from the Burke Chair section of the CSIS Web site (http://www.csis.org/program/burke-chair-strategy). Cordesman formerly served as national security assistant to Senator John McCain of the Senate Armed Services Committee, as director of intelligence assessment in the Office of the Secretary of Defense, and as civilian assistant to the Deputy Secretary of Defense. In 1974, he directed the analysis of the lessons of the October War for the secretary of defense, coordinating U.S. military, intelligence, and civilian analysis of the conflict. He has also served in other government positions, including at the Department of State, Department of Energy, and NATO International Staff. He has had numerous foreign assignments, including postings in Lebanon, Egypt, and Iran, and he has worked extensively in Saudi Arabia and the Gulf. Cordesman is the author of more than 50 books, including a four-volume series on the lessons of modern war. His most recent works include Iraq's Insurgency and the Road to Civil Conflict (Praeger, 2007), Lessons of the 2006 Israeli-Hezbollah War (CSIS, 2007), Iran's Military Forces and Warfighting Capabilities (Praeger/CSIS, 2007), Iraqi Force Development (CSIS, 2007), Salvaging American Defense (Praeger/CSIS, 2007), and Chinese Military Modernization (CSIS, 2007). Cordesman has been awarded the Department of Defense Distinguished Service Medal. He is a former adjunct professor of national security studies at Georgetown University and has twice been a fellow at the Woodrow Wilson International Center for Scholars at the Smithsonian Institution.

operate in a much broader context. They need to know what the civil authorities are doing. They need to work with law enforcement and police. They need to work potentially with things like the public health services. To do this, you need to break down compartmentation. You need to avoid the horrifying tendency to over-classify which seems to be one of the few universal human values. When in doubt keep the secret no matter how much anyone else needs it. This is a challenge for all of us. And it is a challenge not only within countries, it is a challenge within alliances. It is far easier to talk about coordination than it is to create the structures which make it both possible and functional.

I think the creation of common counter terrorism centres that force you to bring together all the elements of intelligence, which bring in law enforcement, which bring in response. The breakdown of artificial bureaucratic barriers and classification is absolutely critical. If you have not done this, you have created the recipe for failure. If you have not practiced it in operation you will probably fail the first time you encounter a truly serious challenge. When we talk about counter terrorism, it is not simply a military task, it is as much a problem of deterrents and response as it is active defence.

In a truly horrifying incident, many countries lack the civil capability to respond to the consequences of acts of terrorism. Biological warfare is a very good case in point. If you are not organizing your intelligence structure to support that response already, you will not be able to improvise in the narrow timeframe that would be involved in something like a serious biological or nuclear or other critical infrastructure incident.

Let me also say here, and perhaps my colleague will focus on this in more depth: two things about what I mean by practice. If you do not practice with the actual architecture, if you do not test the functioning system you have not practiced. These are not academic exercises; these are not scenario studies for war colleges. You are either making a system you have actually tried and tested, or you are kidding yourself. You will produce false-positives or false priorities. This is particularly with the use of computer and information structures. These are a recipe for failure unless they are actually and constantly tested, and even when they are. As we saw in the attempted attack on Detroit, the systems can break down either because of internal problems for the human interface.

This, I hope, is an obvious point, but it has been drummed home to me the hard way since 2001 because I have worked with the US, I have worked with countries in Africa and Latin America and in the Middle East. None of them have had common requirements either for military intelligence or counter terrorism intelligence. What I have said and I say it again: one of the first priorities is to be able to support the police and paramilitary. You do not want to put the military first if you can use normal law enforcement and paramilitary. But they often lack the assets, the intelligence capabilities they need. The best intelligence is often in the military. But then other variables become critical. Does the terrorist group have a secure base because of ethnic or religious or tribal or other support? Is it being hosted and supported by international movements or by a foreign country? Are you working with an alliance? If so, the rules change again. Are you dealing with terrorism in the real sense of the word terrorism? Or with a separate ethnic or religious or other group within your society which challenges national unity, sometimes for legitimate reasons. But calling them terrorists does not allow you to react to the remotest behaviour. That is why the level of popular support for what we call terrorists is critical, as is their level of influence over the population. In most NATO countries, if not all, this is not an issue, but in many countries where NATO may be involved, it is critical. Where the government is not legitimate, calling its opponent's terrorist does not solve the problem or characterize the intelligence task.

And the last point I will make with this slide is, if there is a lesson here on behaviour it is basically small hierarchical groups are easy to defeat, popular movements are not. No one has a common definition of terrorist. Even the United States government cannot agree how to count a terrorist incident. But there is, I suspect, something American with these figures, which are taken from the US Counter Terrorism Center. Why? Because we count every incident in Afghanistan, in Iraq, in Pakistan as international terrorism. What we do not count is serious domestic terrorism in many countries. This is endemic. The question of how you define the terrorist, how you react to it, is it a terrorist not an insurgent, is it a threat or not. Military intelligence has to resolve this. And it does not matter whether we call them terrorists. If they are asymmetric threats and they use terrorism or they use intimidation as only one tool, they still have to be dealt with much the same way. That is why it is critical to get your priorities right. If you can stop this by military support to paramilitary, legally, you are far better off than letting it escalate. But if you cannot, you run into major problems fairly early.

Let me note here. If there is prior experience as to what can go wrong, it is not simply ignoring the threat. Many paramilitary forces are corrupt or incompetent for these missions. The same is true for many reserve forces. They were not designed for these tasks. If they are armed and if you cannot solve it legally, you may have to switch to the conventional military very quickly. Simply because they have the discipline and integrity. And that is why again characterizing this by country is critical to defining the military intelligence role. But once it escalates it becomes a very different situation. The truth is that we like to call insurgency terrorism. Unfortunately, when you do, the label does not describe the task. And once it escalates to that level, military operations have to take on the character of a very direct intelligence support, tailored to different types of roles and missions. And in simple terms, they are part of what we have chosen to call full spectrum or hybrid warfare. That is fine in theory as a label. But the problem with it is, you have to figure out what it means in practice. And as we look at this, what we have learnt in Iraq, what we have learnt in Afghanistan, what we should have learnt in Vietnam, what we have seen in Columbia and countless other cases, is, you cannot win those wars by military means under most conditions. The military has to work with governance, it has to work with aid; it has to address the population while it simultaneously has intelligence support to attack the threat. But that means the intelligence task must cover the civilian population. It must understand how the action of the military, the government and the civil side is perceived by the people. If we look beyond the threat and listen to what is happening in the field, it must listen to the aid workers, it must listen to the small units operating in the field. It must listen to the people attempting to make governance work; and it has to listen to allies. Because the moment we separate operations, as to some extend we have in Afghanistan, we cripple the intelligence task and we cripple the effectiveness of the mission.

Now, we talk about this in practical terms as full spectrum operations. Let me note here, the United States has spent now nine years trying to figure out how to reshape intelligence assets to do fundamentally different tasks, to support a whole range of government approaches as well as military operations. I cannot get into the full range of changes here. But it is critical that you look at all your assets and all your major forms of collection, information systems and analyses. It is equally critical more and more that you open up the military to look at tools like open-source data, human terrain mapping and polling. You see these critical ways to learn the population and popular perceptions. It is also critical from some of the exercises I have seen, to understand the role of the military in dealing with critical infrastructure protection. If you have not tailored your military structure to respond to critical incidents, or infrastructure destruction, there is no civilian alternative. You open up key aspects of your country, economy or society to the threat.

Now, very quickly because these are issues that I could spend a long time on. The targeting intelligence design for a regular military operation is the perfect way to lose in counter terrorism or counter insurgency. You must have a fundamentally different level of targeting. You must focus on collateral damage, you must focus on civilian casualties, and you must focus on popular perceptions. And you must calibrate what you are doing in terms of whether you are winning rather then destroying the enemy. We failed to do this early in Iraq. It took us some years to adopt. We failed to do it in Afghanistan for nearly eight years. And the price was almost immeasurably high in empowering the Taliban.

One of the lessons we have consistently learnt from Afghanistan is it was not the presence of foreign troops that Afghans resented. It was two things: it was first civilian casualties particularly from air strikes and artillery, and second, the failure to understand the technical victories that abandoned the people, that left them open to the Taliban, were dismal failures, because people saw no reason to regard the military as their protectors, as distinguished from the threat. We have seen similar results in other countries including Iraq.

Again, moving very quickly is aware of using extremely expensive toys. There are some countries, which are rushing to acquire remotely controlled aircraft and combat vehicles. What they do not understand is, as is the case with many intelligence assets, if you do not have enough of the assets and enough of the people to use them properly, they actually blind you to establishing the military intelligence present with things like Special Forces on the ground. The person with the most toys does not win. The person with the best mix of military intelligence asset does.

Another critical problem here, one of the ones, which perhaps we have made the least technological progress is understanding the impact of military strikes. Now, these core actions, this may or may not be a military intelligence task depending on the country. Let me say it again and again. Two things happened: first, the battle damage assessment grossly exaggerates what happened. In terms of the number of terrorist killed, the number of terrorists dispersed, the damage done by an air strike, the damage done by the use of a missile. Very often there is confusion between blowing up a building, and knowing what is inside the building, and knowing what killing a given group or unit may do. We need to fundamentally reassess battle damage assessment both to be sure of the results of asymmetric and regular warfare, and, as was pointed out earlier today, to understand these are forms of strategic communication. When you kill people, deprive them off their living, drive them out of their homes and blow them up, you have sent a very powerful message in strategic communication. It is not in general message in strategic communication. It is not in general the one that defeats terrorism or insurgency.

The last point in terms of function: I hope this is clear to everyone; it is certainly a lesson the United States learnt the hard way. Whether this is a task for military intelligence again varies by country, and the role of civilian intelligence for security forces and paramilitary forces also will vary by country. But let me say that what happens, when you abuse the military system and the role of military intelligence, is almost invariably you create more terrorists than you destroy or interrogate, and you basically alienate people into becoming terrorists that otherwise would not become terrorists. People debate this. This is my position, but I hope it is a clear one.

Finally, what we do with this, we need to look at this in assessment terms. We cannot separate intelligence from plans and operations. We cannot separate the military from law enforcement and civil law and order. Either as a country or as an Alliance we need to integrate our efforts, we must not create a situation where military intelligence follows and supports operations and plans, but plans and operations do not have the intelligence support to either defeat terrorism or prevent it from escalating to insurgency.

So just to conclude, fusion is everything. Begin by using military intelligence to support the police and paramilitary where this is possible; address the full range of tasks; understand the need for quick reaction civilian-military programs; focus on winning the population not tactical encounters or killing terrorists; focus on key figures rather than the broad structure of terrorism so you can attempt to destroy the network; but above all understand the role of military intelligence. Like military operations it is to shape the population's rejection of terrorism and insurgency. It is not to conduct operations as if the people were part of the landscape and could somehow be ignored.

Thank you very much!

Assoc. Prof. Wesley K. WARK (CANADA)*

"Intelligence Coordination In Countering Terrorism"

Ladies and Gentlemen,

It is a great pleasure to be here. I want to extend particular thanks to Colonel Çelik who actually made it possible that I am here after my original flight was cancelled and he managed to find a replacement in the early hours of Sunday morning, I am very grateful for all his efforts. He is an artilleryman clearly cool under fire.

My task today is intelligence coordination in countering terrorism, and I should begin by saying, I hope I am not here under any false pretence, I do not know if there are any Canadians in the audience, but let me say that Canada has no particular advantage or place in terms of trying to solve this problem. In fact, it is an endemic difficulty for us and our intelligence community as it is I think for every intelligence community with which I am familiar.

My mantra really is that intelligence coordination in countering terrorism is an old problem in a dramatically new phase. And I want to spend a little bit of time on the history of these old problems so that you can appreciate the argument, I am going to make about the nature of the new phase. So, here is a little bit of history. I hope you bear with me on this. Intelligence services, I would argue, have been confronting problems of coordination since they were born. Modern spy

* Wesley Wark is an associate professor of history at the University of Toronto, teaching in the international relations program. Professor Wark is one of Canada's leading experts on intelligence and national security issues. He is a Past-President of the Canadian Association for Security and Intelligence Studies (1998-2000 and 2004-2006). He serves on the Prime Minister's Advisory Council on National Security and the Advisory Committee to the Canadian Border Services Agency. He is currently completing his book on the history of Canada's intelligence community in its formative years from the end of World War II to the height of the Cold War, and a study of contemporary Canadian national security policy and counter-terrorism. He is also the co-director, with Mel Cappe, of a research project on "Security and Democracy," funded by the Institute for Research on Public Policy. Professor Wark is a frequent commentator in the media on security and intelligence issues and is a regular book reviewer for The Globe and Mail.

agencies in the real sense of the word were only created in the years before the First World War.

Let me give you an example of this early difficulty. The predecessor organization of the modern British intelligence community, the British security service and the secret intelligence service were created in 1909. In essence in 1909 the British intelligence community consisted of two people Vernon Kell in charge of internal security and intelligence, and Mansfield Cumming who had been given the task of starting up an oversees intelligence gathering enterprise. One might think that a two person intelligence community could manage coordination and cooperation, but in the British case, in this case, they did not. There were right in the beginning quite vicious battles over their respective mandate, over defining the boundaries of these mandates. They were over budgets and in fact they far over who could use the only office safe that they were given by the treasury in 1909. So the British, I suppose could be supposed pioneers in the invention of bureaucratic turf battles over intelligence. But just to present a reasonable picture of a historic record, I think the British also have to be given credit for an early appreciation of the importance of intelligence coordination and cooperation. And that early appreciation took concrete form in the creation of something called “The Joint Intelligence Community” which was created in 1936 as the British Intelligence Community began to become a bit more concerned about developments in Europe and the threat caused by Nazi Germany. And of course this Joint Intelligence Community or JIC remains in being as a high-level intelligence coordination and threat assessment community to this day, and in fact has served - I would argue - as a model for many other endeavours around the world, including in the United States, my own country Canada, in Australia, and elsewhere. And perhaps you have something similar here in Turkey.

So really, in terms of problems we could talk a lot about the history of intelligence coordination problems, but I think the underlying message is that intelligence coordination has long been recognized as a problem, and the solutions have been long looked after, but have remained by and large elusive. One of the ways in which solutions have been looked after I think goes to the heart of questions about how intelligence communities have been structured, and then particularly the question of what is the best model. Is a centralized intelligence system – kind of top-down hierarchical command and control oriented – the best way to get good results out of an intelligence community or rather a more decentralized system, which is often called “cycloid intelligence community”, that recognizes special expertise. Is that the way to go?

At the heart of these debates have always been the issues of structure and organization, which can be very boring debates, but in this context, I think, very important ones, that hold the answer to the question of getting coordination working. But what I really want to focus on today in these brief remarks is the new phase of intelligence coordination and the new challenges, in particular in the context of confronting terrorism.

Let me begin with a set of remarks. None of which will strike you as original, but may be need to be laid down quickly. One is that in a post-9/11 world, in the 21st century world, we are living in a new and complex threat environment. There are new and vastly large expectations around intelligence performance as a preventative weapon. And to compound all this, I think the intelligence communities bear a heavy burden of failure. In terms of their performance since the 9/11 attacks, there have been intelligence failures, intelligence failures regarding the attack, regarding Iraq’s weapons of mass destruction. These are only the two most well-known famous examples of under-performance on the part of intelligence communities in the phase of these new expectations, and this threat environment.

Part of the reason I mention this is that in the aftermath of this, the series of failures on the part of intelligence sparked a lot of criticism and good ideas how to solve the problem. Here is an idea of a simple solution to this intelligence coordination problem. This simple solution goes by the name of “connecting the dots”, and basically the idea is that if only intelligence communities could simply get their act together and connect the dots, then we will have the kind of perfect intelligence picture that everyone wants, and all would be well.

The most recent example of – if you like – the deployment of this idea, this language of criticisms of intelligence community performance came in the context of – I think Anthony mentioned it – the attempt on Christmas Day by a Nigerian, the so-called “Christmas Day Underwear Bomber” to blow up a flight on route to Detroit. The Canadian media was fixated by the fact that if he had succeeded, it would have blown up over Canadian territory, but I am not sure that that was really the most significant aspect of this. The important thing in this regard is, that again there had been a failure to connect the dots. So what if we examine this idea of connecting the dots, what it reveals about the challenges of intelligence coordination in this long war against terrorism. But again I want to stress that the very idea of connecting the dots can be overly simplistic and even dangerous. Overly simplistic because especially counter terrorism, if you think about it, the dots can be more or less invisible. The picture that you are trying to put together is rarely clear, rarely aesthetic, and generally does not exist in one particular, or is confined to one particular geo-political space. The connecting-the-dots idea is also dangerous for a couple of reasons.

One is that if the wrong dots are connected, innocent persons can be seriously affected. And in Canada, I am sure we are not unique in this regard, we have had a whole strain of highly publicized cases where Canadian citizens have been wrongfully suspected of involvement in terrorist activities since 9/11, and found themselves imprisoned and tortured oversees in Middle East countries. National security doctrines and statements of intelligence strategy released in profusions since 9/11 repeat that over and over again. The mantra has been need for coordination, integration of intelligence; essentially they are binding into this idea that it is about connecting the dots.

A recent example would be the United States National Intelligence Strategy released by the Director of National Intelligence in August 2009. Its vision statement describes the need for the intelligence community to be integrated, a team making the whole greater than the sum of its parts. It talks about – and I am just quoting some pieces of the language here – improving collaboration, sharing information, creating a unity of effort, enabling information flows. It looks to the genie of technology to achieve this, while worrying at the same time, appropriately I think, about information security.

All of these are fine words and goals, but let us look a little deeper at what this all means. There is a wonderful piece, I think written by a writer who does not usually enter into this world of intelligence and terrorism, a writer with the name of Malcolm Gladwell. He might be known better for his books on the “Tipping Point” and “Blink” and all manner of things. Did I say he was Canadian by birth? He wrote a piece in the New Yorker magazine which is entitled “Connecting the Dots”, the problem of intelligence reform. In this article, he dissected the idea of connecting the dots and founded a false idol often driven by what he called “creeping determinism”, that the picture should have been seen that we later created retrospectively. Forgetting all the while the wonderful lesson Roberta Wohlstetter first taught us long ago in our study of Pearl Harbor that with any kind of intelligence crisis, what you will see is a confusing combination about true signals and false noise.

As for Gladwell he believes, as I do, connecting the Dots idea fundamentally misrepresents the complexity of the intelligence problem. He also points out the fact that connecting-the-dots thinking can contribute to a temptation on the part of seeing your policy makers, even seeing your intelligence chiefs to demand a relatively simple solution, also with respect to the nature of any particular threat. One of the most prominent examples of this of course occurred in the run up to the 1973 Yom Kippur War. On the eve of that war the chief of Israeli military intelligence saw it as his duty to deliver a simple yes or no to what was a complicated question, as to whether Egypt and Syria were preparing for war. His answer, as I am sure many of you will know, was a fateful one. They found out otherwise in the couple of days to come.

The demands to connect the dots in fact are an enemy of intelligence's true mission I think. That true mission is not to be simple but to be complex, not to be certain but to be nuanced, and on occasion to be prepared to confess that you, as an intelligence community, simply do not know. You do not know the dots; you do not know how to connect them.

So let us consider for a minute the broad purpose of intelligence. It is about delivering knowledge and sometimes warning about threats. It has traditionally delivered that knowledge and warning through monitoring at least state and non-state human actors and putting aside all those other kinds of threats that deal with, it concentrated on essentially two categories of knowledge. It concentrated on capabilities, and it concentrated on intentions. I want to just pause and think a little bit about the history of the intelligence communities' work on those two issues: capabilities and intentions. But in the run up to World War II, the capabilities and intentions of Germany both alluded the intelligence services of all of Hitler's adversaries.

During World War II the focus became increasingly simply the military capabilities, partly because the question of what Hitler's intentions might be, ceased to be adventurous. The British and American Intelligence Communities in particular became quite good in the measure of military capabilities, something that was vital to the success for example of the Normandy invasion of June 1944. Without good intelligence that invasion could not possibly have succeeded. In the Cold War the intentions of the Soviet Union and its allies sometimes, often, proved inscrutable. Again the effort to measure capabilities came to the forefront and again primarily, in military terms. It was something the United States Intelligence Community got very good at, not least because they were able to generate and deploy very technologically sophisticated and innovative new intelligence platforms starting with the U2 spy plane in 1956 and going on from there.

But I would argue that a new phase of coordinating intelligence is coming in the context of terrorism. I would argue that the phenomenon of trans-national or globalised terrorism has turned intelligence experience, and turned the general intelligence practice upside down. What I mean by this is to say simply that, if intelligence and capabilities are the two key challenges when it comes to terrorism groups and understanding a threat, intentions are now more knowable than capabilities. The capabilities' side is really the hard part. So we reversed the equation. We can know intentions, may be that is easy. We find it very difficult to appreciate capabilities when we describe and define capabilities very broadly.

The 9/11 Commission Report faulted the US Intelligence Community for arriving, among other things, at wrong conclusions, for suffering, among other things, a failure of imagination. That is a much contested idea in the aftermath of the release of that report. But this is one that I subscribe to. I think the notion of failure of imagination is a very important one. That failure of imagination that the American Intelligence Community suffered was a failure to appreciate not the intentions of Al-Qaeda but the capabilities of Al-Qaeda. The problem of measuring terrorist groups and terrorist's individual capabilities persists. If we are going to measure those capabilities, we come back to the question of connecting the dots. Now we are trying to connect the dots, even if this is a false and misleading analogy or false idol, it is not going to go away. We are now talking about this principally in terms of capabilities. If intelligence communities are going to get good at understanding the capabilities of terrorist groups, they have to, in my view at least, fundamentally reconfigure themselves and transform themselves, because again the capabilities versus intentions, hard intentions versus easy intelligence issue has been turned upside down in the 21st century world. And here, I kind of happy and frustrated overlap with what Anthony Cordesman has to say.

In terms of how intelligence communities need to transform themselves to deal with this capabilities issue with regard to terrorism. Let me say that I think there four things that are underway. All of them are more promising than others. There is a greater demand for intelligence sharing and cooperation across agencies within governments across the civil military divide within governments, across the so-called Chinese walls that separate intelligence from law enforcement agencies in many countries.

There is secondly also a greater demand for intelligence sharing and cooperation pushed through various levels of government. From the top level, whether it is a federal system or some other system, down to the local or municipal level. And in doing this, it creates many new consumers of intelligence, but then, it also creates some useful new suppliers such as local police forces.

Thirdly, there is a greater demand for intelligence sharing and cooperation beyond government to push this whole enterprise of intelligence, if you like, out into the public domain. And it is in particular focused on a need, perceived need, in some intelligence communities at least, the need for outreach; to reach out to the private sector and to academia for expertise they may not be able to generate themselves.

This is something that I have had a lot of experience with and I find intelligence communities largely resistant to, indeed some of my academic colleagues also curiously resistant to. And then finally in terms of transformative pressures, there is - and I think this is really the most important and significant one, and I come to my overlap with Anthony's paper – a much greater demand for intelligence sharing and cooperation with foreign partners; to move intelligence from what it had always been from the moment of its modern birth before World War I down to the present, from a strictly national focus to something much more multinational, if not international, as an enterprise.

I want to talk a little bit about fusion, and what fusion might mean in this context. And I love this clock, and I have a minute 41 second to go. Fusion seems to me one of these ideas that has emerged as intelligence services try to comprehend the new threats posed by terrorism and try to transform themselves. And the idea behind fusion is simply that if you can construct new kinds of intelligence organizations within your community, that are meant to be fusion centres, it might become and advantage and a lead and an edge in terms of the capabilities problem that I have called your attention to.

And of course there are a number of fusion centres for counter terrorism work that have become bigger throughout the world since 9/11. The national counter terrorism centre in the United States was the pioneer in this. The British followed with JTAC the joint terrorism analysis centre and Canadians were always good allied followers in this regard. In this regard it created its Integrated Treat Assessment Centre in 2004. The idea is that fusion centres would be a structural note for all source collection analyses and threat reporting focused on terrorism. It is a nice idea; it is an idea that responds to this idea and this requirement to connect the dots. But I think fusion centres as an experiment are perilously close to being thrown on the junk heap of history. Partly because they have not given time to work, partly because they have suffered evident failures, partly because I think when they were first set up, there was no real recognition of what they would need in terms of capabilities in order to succeed.

So I am going to finish this talk on fusion as a possible solution to our problems and capabilities in connecting the dots by suggesting what the shopping lists for fusion centres really are, if you have one, or if you are thinking of setting one up. I have been very critical of the Canadian effort in this regard, but very hopeful that the Canadian effort will ultimately succeed. You need expertise, second you need real resources, third you need a very technologically sophisticated information sharing platform; forth and this is difficult, almost from the outset, a good reporting record so that you can prove the experiment is worthwhile. Fifth you need outreach and intake capabilities, that business moving out into the public domain, into the private sector, to vacuum up expertise. You need information, security and resilience.

But above all, and I think this is the only reason why the experiment should continue and the reason why we should have some hope in it, as a partial solution as we go down the road to this very complex terrorism threat. Fusion centres are the best hope for a genuine international cooperation in terms of counter terrorism work. They may force recognition that the real effort in genuine coordination involves the creation of sustained international networks of connection analysis in reporting.

And the least, we are a long way from that goal at this present moment.

Thank you!

FIFTH SESSION
QUESTIONS AND ANSWERS

Q: General Hayrettin UZUN: Thank you very much. Retired Lieutenant General Hayrettin Uzun; as it always been a very interesting speech has been given here by Mr. Cordesman. And because of his wide experience, I would like to ask him to enlighten us on one subject. General McChrystal in Afghanistan is the responsible person in charge and that as a result all information reaches him, tactical, operational, strategic, asymmetric, combat and also against terrorism. Do you think that this multitude of information makes it difficult for the commanders to decide? Are you considering a new work or solution on this aspect in Afghanistan?

A: Prof. Dr. Anthony H. CORDESMAN: I was directly involved with McChrystal when he first went to Afghanistan, when he shifted from what was in many ways tactically-oriented strategy to a population-oriented strategy. It did not mean that he gave up tactical operations against the enemy, but it did mean that he recognize that the protection of the population, the creation of secure population centers where you could bring in aid workers, government agencies, police, the rule of law was absolutely critical to holding the Taliban at bay. We were winning virtually every tactical encounter in Afghanistan and losing approximately 20 percent of the country between 2005 and 2009. As a result General McChrystal fundamentally shifted the structure of the intelligence effort inside Afghanistan to focus on population, attitudes, that are very local as well as regional, and on the national level to support aid workers, to work in terms of efforts to bring local governance either through the Afghan government or through local, tribal leaders. And under Major General Flynn whose actions are to some extent public, you see a fundamentally different approach. You would not reject it in any sense, the need to support military operations. But you have to make military intelligence part of the fusion, as my colleague defined it. But fusion in terms of cooperation and sharing data between very dispersed groups with different functions where you cannot connect every dot. But everybody needs a common level of situation awareness and support. Now some of this sort of modelling is becoming public. There is one article by the NAUS think tanks that is on the web. And as I speak you see similar exercises to fundamentally zero-basis going on both in Afghanistan and Iraq. The United States is really reshaping its analytic models, and they are models which serve every one and where you have a holistic government approach. Because I think every problem that was raised in the other presentation can be all too real if you feed the high command, but you do not feed the troopers in the field.

Comment: Prof. Dr. Yonah ALEXANDER: Anthony Cordesman correctly tried to focus on the practical approach. All of us, I think, we are trying to see the forest but also the trees. I would appreciate some elaboration on a number of interdisciplinary perspectives. Number one on the historical: what are some of the historical lessons in terms of success and failure that worked, what did not? Secondly, on the sociological perspective in terms of the role of the civic society in relation to intelligence. Three, in relation to the art issue, whether we are talking about a photo or a painting or music, in relation to intelligence? And four, in regard to communication. Anthony you referred to its strategic implications, in other words, without intelligence, as some of our colleagues remarked, there is only noise. And intelligence without communication is irrelevant. And finally, number five, on the legal perspective in relation to the suspects, early suspected citizens. Thank you!

Q: Brigadier General İlyas BOZKURT (SHAPE Director Intersupport): My question has to do with the first speaker's introduction. When I read Major General Flynn's ISAF CJ2 fixing inter-paper, two questions occupied my mind. First, he was offering a wider level of intelligence sharing, info sharing in ISAF. The question was, if the US Intel Agencies are ready to support Major General Flynn's initiative. To be more clear, are they ready to make more information or intelligence available to NATO. The second question was how can we find a right balance between higher levels of intelligence sharing and protection of classified intelligence or information? Thank you!

Q: Esef MERDOĞLU: I would like to thank you. Esef Merdoğlu, I am representing Asker haber.com in Ankara. My question is directed to Prof. Cordesman. Prof. Cordesman at one point in your speech, you referred to incidences that took place within the boundaries of a country, is that insurgence, terror, or what? You said "we did this in Colombia, we did this in Vietnam. Bu we learned our lesson and did not do it in Afghanistan and Iraq." If 9/11 had not taken place, many of the countries fighting against domestic forces, would they have been on the international list of terrorist organisations published by the United States every year? And intelligence, could there have been such a wide integration in intelligence otherwise? Thank you.

A: Prof. Dr. Anthony H. CORDESMAN: Let me try to take these very quickly with my Canadian colleague, the ability to provide wisdom as to distinguish information, frankly every major strategic event changes the way national security communities' respond. 9/11 has changed the behaviour. Now, if you look through the list of terrorist organizations however, in the open source US material - it is not particularly sophisticated - the State Department's view on terrorism looks like it was sort of turned out of yesterday's computer memory, other than updated. I think that you would find the intelligence community does look at these individual groups. And some doubt, but I will be very careful about the thing that the US' open literature is anything like what it should be. That unfortunately the invention of the computer allows governments to keep reports, repeating virtually the same report with minimal changes. If what happened had not happened, I do think, we would have calmed down; but not after such a cataclysmic, dramatic event. But we would have found ourselves faced with some equivalent that would have driven us to deal with counter insurgency and counter terrorism, simply because the forces are much broader. In one way or another if it had not been 9/11, something else would have happened. A threat to Saudi Arabian oil resources, a major problem in Europe, some other attack would have occurred.

We would have been somewhere close to where we are now. Let me say in terms of General Flynn's terms of intelligence sharing, I think when you are at ISAF Headquarters, you already have a pretty good level of intelligence sharing and much more information flow. That has heavily increased in 2005. But having been in NATO headquarters and having been involved in the past with the MC161 exercise, let us face it. Every country wants to have as much of the other country's intelligence assets as it possibly can get regardless of whether NATO necessarily needs them or not. The politics of intelligence are collected from your allies or your enemies, so there is always going to be a balance between what countries do and do not release.

I think quite frankly looking at some of the flow, there are countries in the alliance which are so sensitive to their domestic politics, that they are considerably less willing to release data on internal problems than the United States. We will not see a quick change here. In terms of the balance of security versus release, the rule I always had is bit of a very simple one. If you cannot tell where they should be classified a week from now it is not secret. The problem is it is almost exegetic; you stamp the damn thing "secret" on everything. And if you control a department you want that department to give you power. So you have to be afraid to actually release it. And you have to be afraid if you are at the centre to stop trying to use your access to the President or the Secretary of Defence or the Chief of Staff to control the flow of data that you should really be giving out not only to the theatre commander, but often down to the captain or lieutenant in the field. And fighting that battle is at least as constant as getting things being unclassified. And I have to say we have made real progress in the US, but frankly not enough progress to help. Did you want us to go on to the last question which I think was the first question which touches on both of us? Right!

General, let me just say very quickly. There are so many different types of failures and success in intelligence that I do not have the time to even begin. Just in terms of what happened in Vietnam, however, I will tell you what is the most critical problem. It is the natural tendency of people to delude themselves. To support the mission, to support the politics, to support whatever is now being done, to go on doing what they have done in the past regardless of whether it is relevant. To call attention to themselves by over-dramatizing the product or delivering a message by oversimplifying it. It is not some sort of dramatic failure.

The second point is, when in doubt you blame the intelligence community, so you always have a false model of intelligence and it always shows you did not connect the dots. Its anthropology, its politics, its human terrain mapping, but we are down to the end of a dark and narrow valley in terms of these activities in Afghanistan versus 17 different groups in a place like Kandahar. And you have to look at this in human terms in a very broad political sense. It is intelligence and art rather than science outside of textbooks, everything is an art. Even particle physics. I mean calling it science to give the level of practice dignity beyond all credibility none of us have gone from art to science in the real world. Strategic communications, I would just close with one point. Again, strategic communications as we have heard this morning focused on one of the most critical tasks we faced. But the way governments communicate most is by how they use force whether they govern well, whether they are corrupt, whether they serve their people. I do not care how good the message is, if you are not protecting the people, if you are not delivering good governance, and you do not give them a working economy and hope, nothing else by way of strategic communications is really going to deal with the problem.

A: Assoc. Prof. Wesley WARK: I will do something that the intelligence community was never supposed to do which is cherry picking from this list. Just a couple of things, and I will keep this brief. One of the questions that the first individual, sorry I do not know your name, raised was historical lessons and it is probably important to say that it is not necessarily the case that history has anything particularly valuable to teach us. But in terms of historical lessons I think, we now have accumulated a lot from intelligence experiences and read a lot about it. It is maybe easier to say why intelligence fails as opposed to what makes it successful. The intelligence systems which never work, never worked in history, are over-centralized intelligence systems. Political structures in which political leaders either pay no attention or have no respect for intelligence. And above all this is kind of a Prof. Cordesman remarks: what we want is an intelligence community which is capable of free thinking and capable of constantly contesting its own views; no easy thing to do.

On the civil society question, this is an important issue and I would just say that what we want ideally is for the public to both understand and respect the work of intelligence communities. Very hard job! Made slightly more difficult by the kinds of images that pervade in popular culture which provide a great deal of what they think and know about intelligence? But the key is respect and understanding. That does not mean that societies should not be; do not need to be critical about the work of intelligence communities. But they have to respect that criticism and understanding. And intelligence communities have to be sufficiently aware of the fact that they need public support to make them want to do their job well. There was a question raised if I understood it rightly about how you deal with, if you like, legal rights, in the context of war and terror. Here I will sound like I am channelling President Obama, but I think the basic truth is that whether it is intelligence communities or any other aspect of a counter terrorism effort, you have to maintain the rule of law. And you have to maintain the feasibility of that support of the rule of law. And we have gone down clearly some very wrong paths in that regard which have come back to haunt both the intelligence community in terms of performance and society's respect for that community.

I was going to say something about the General Flynn report, and the question of sharing intelligence. But I have just time to say that if anyone wants a lesson on how to collect intelligence from their allies you should look at Canada which is a net collector of intelligence on its allies. Thank you!

THIS PAGE IS INTENTIONALLY LEFT BLANK

CLOSING REMARKS

GENERAL OVERVIEW

Prof. Dr. Ersin ONULDURAN
Ankara University

CLOSING REMARKS

General Aslan GÜNER
Deputy Chief of Turkish General Staff

THIS PAGE IS INTENTIONALLY LEFT BLANK

Prof. Dr. Ersin ONULDURAN (TURKEY)*

"General Overview"

My Bio data did not say for how many years I have been married, I have been married for 41.5 years now. And I believe that is a success; so just I wanted to inform you. I took a lot of my notes in English.

And as a lot of the speeches were made in English, I thought I would first make some notes, and then share some of my thoughts with you.

But to lighten up the mood, if I may, I would like to tell you a little joke, following suit of our American and Canadian speakers in the earlier sessions. As things often happen in the American countryside, there was a driver. He is going by car and he sees something flash by. He looks around and he sees another one of these things flash by. And he stops by a house he says, "Excuse me, sir" to the occupant of the house. "Is that a three-legged chicken that I saw just flash by." The owner of the house says, "Yes, indeed. It is a three-legged chicken." "Well, how does a three-legged chicken taste? And why did you raise these with three legs." He said, "I like chicken legs, so does the misses. When junior came along we decided to raise them with three legs." The friend said, "How is this chicken? What does it taste like? Tender and nice?" He replied, "Damned if I know. Never been able to catch one."

This is in fact my third year, I have been fortunate enough to be able to participate in these sessions my third time. I am happy to see that our three-legged chicken, terrorism is in fact something that we are almost ready to catch.

* Born in Bandırma in 1945, Prof. Ersin ONULDURAN was educated at the Claremont Men's College (B.A. in political sciences), the California State University (M.A. in international relations) and the University of Southern California (Ph.D. in political sciences). He began his work as a research assistant at the Faculty of Political Sciences of the Ankara University in 1973. He received his associate professor and professor titles in 1983 and 1989 at the same Faculty. He is currently the head of the Department of International Relations and the Director of the School of Foreign Languages at Ankara University. In addition, he has been working as the Executive Director of the Turkish Fulbright Commission since 1986. Prof. Ersin ONULDURAN is married with one child.

In other words, now as compared with nearly six years ago. When we first started these sessions, there was some debate as to what constituted terrorism, what kind of actions were terrorist actions, what kind of actions were movements of national liberation and so forth. But now, there is a litmus test. If there are civilian casualties, if there is a threat of use of force, and maiming and killing, and when innocent bystanders are victims then that is definitely terrorism.

Now, what are the causes of terrorism; what I am going to take away from this meeting this afternoon, is, that it is very varied. The commander of the Turkish Armed Forces set the tone; General Başbuğ set the tone when he told us a number of things that were quite interesting to me as an academic. One of the things he talked about was that gathering of intelligence and making sense of intelligence across different agencies and across countries has become of extreme importance. In fact, this is one of the issues most of you will remember. Between the United States and Turkey that was resolved with the so-called actionable intelligence that was shared, and that caused or resulted in certain successes of the Turkish Armed Forces in actions against PKK terrorist activity in Eastern and Southeastern Turkey.

Another thing that I am taking away this afternoon is that we have to listen what the terrorists are saying. Not so much as to understand their message, but in order to be able to analyze what it is that they finally tell their own people, and how we can get in the hearts and minds of the people that we are trying to win over; that we have to win over if we are to win this war against terrorism.

The other threat that definitely scared me, what I thought was somewhat manageable, is the inevitable nuclear - and later on I learnt - biohazards that are imminent, and in fact I recently read the memoirs of George Tenet, the CIA Director who was the director of the Central Intelligence Agency under two administrations. He said in his book, he was asked by one of the people who interviewed him, "what is it that you lose sleep over?" He said, "I lose sleep over the possibility of a dirty bomb, of a nuclear device being exploded, a small device if you will, in the middle of Manhattan, in the back of a truck, and untold casualties that it could cause." This was something to us uninitiated civilians that is a scary thought. But it is not unmanageable. With increased vigilance, and with increased money and efforts spent and the control especially of the large containers that pass through big harbors such as the New York Harbor. I think this is being brought under control, and it is a somewhat manageable risk that we can all take.

A question that remains “is terrorism religiously motivated?” My answer here would have to be a resounding “No”. Unfortunately, the images are of people with beards, green flags, they squeak to us in writings which often mention the name of God and in the name God violence is committed. Imagine the pain of Daniel Pearl’s family when they saw these images, when this unfortunate event of his killing occurred before cameras in the name of God. Abu Musab al-Zarqawi of Iraq for a long time used religion to justify his terrorist activities. But we must also remember that often a clean-shaven face and blue eyes can also spell terror. We have seen examples of this, and there is terror also in Europe. And there are other examples, like the terrorist activities we saw in Japan, in the massacres at the metro stations. They were not committed by Muslims. So terrorism does not have a religion. Terrorism is terrorism, should be identified as such and should be dealt with as such. In dealing with terrorism, yes, I understand that it has been with us for some time, and perhaps it will be with us during our lifetimes. But are we going to throw up our hands and be defeatist about it? Absolutely not! I think we should hit hard, but you should hit hard at the right targets.

In other words, when we are hitting as far as the war on terror is concerned, and I would like to mince no words here, and use that expression “war on terror”, and this does not have a copyright, what should I say, copyrighted by Mr. George W. Bush. You can call it "war on terror", if it is "war on terror". When you do that war on terror, you cannot dismiss, as collateral damage, all the possible damage done to innocent bystanders. For example, it is prudent to protect your troops and use drones. But at the same time, if unfortunately you also continue to hit partygoers, merrymakers, Afghan wedding parties and so forth, then you are going to lose the local populations and not win the hearts and minds you are very much desperately in need to win over, if you want to win the war on terror.

Finally, one thing that stayed with me after this meeting is something that the Chief of the General Staff of the Turkish Armed Forces mentioned in his opening remarks. And that is that the armed forces are one with the environment, with any sort of environment, just as there is eco-tourism, there ought to be an eco-war, if you will.

Again, the best way to fight the war on terror is to blend into the environment to make use of the possibilities that the immediate environment provides for the forces that you are putting in the field. And you cannot - even in your own country or if you are fighting a war in a foreign country such as in Afghanistan or Iraq - have a scorched earth policy. In other words, one must never lose sight of the fact that it is human beings after all that you are dealing with, and if you win a battle against a given group, you might lose the whole war. If you in fact have a sort of uncaring scorched earth policy that you apply. Do think of the future.

These are some of the thoughts that I have gathered at the end of these proceedings. One fact that also remains with me is that there is a very great likelihood of proliferation. If there is nuclear fuel enrichment, and if it is pursued too energetically. I understand the reasons of countries to try to develop a capability of providing energy for future generations; but balances are extremely important, and nothing should ever be hidden. There is a threshold in the scheme of nuclear brinkmanship. If you pass that one time, I do not know, you cannot go back. Therefore, if there has been one instance of cheating, one instance of finger pointing but you did no show us the X, Y and Z facilities, then I think from that point onwards - whatever nation that is, I am not naming names - cannot be trusted. Therefore, if I were in a position of decision-making, and if I were in a position of developing future nuclear capabilities, I would be extremely careful about obeying the law of the non-proliferation treaty.

These are, ladies and gentlemen, some of the thoughts that I picked out of the proceedings of the past sessions. My final thoughts for you would be let us not lose sleep, but not lower our guard and definitely hit hard at the right targets, at the right time, and at the right place.

Thank you for your attention!

General Aslan GÜNER

Deputy Chief of Turkish General Staff

CLOSING SPEECH

Sir, and Distinguished Guests,

Firstly, I would like to express my gratitude to all who participated, successfully chaired the sessions, and shared their knowledge and experiences during our just-concluded “Third Symposium on Global Terrorism and International Cooperation."

For two days, we have had the privilege of listening to critical observations and evaluations from distinguished specialists and experts on how to fight terrorism while preserving our human rights and liberties, democracy, and shared values. I believe that this exchange of valuable ideas and viewpoints on terrorism has been very beneficial to all the participants present.

During the symposium,

- Various approaches have been put forward concerning globalised terrorism and the role of international law and institutions, intelligence-sharing, technological advances, and strategic communication in the defence against terrorism,
- It was confirmed that the nature of the terrorist threat has been transformed into a real threat to the entire world,
- It was emphasized that the effects of terrorism are not only limited to the countries where terrorist activities take place, but also have an impact on neighbouring countries.

It was concluded that terrorism threatens not only the countries directly targeted but also regional peace, prosperity, stability, and the economy. Should a common stand not be taken against terrorism, its pernicious influence will inevitably continue to spread.

Unfortunately, no single country has the ability to fight against and defend its citizens from terrorism, as it has become an asymmetrical, globalised and multidimensional threat. This has made international cooperation a must in the defence against terrorism. The main objective for cooperation should be to maintain harmony between our words and our deeds. It is crucial that a common stand opposed to every type of terrorism and a common understanding for the safety of human life be developed.

Our great leader Atatürk expressed the necessity for international cooperation in such struggles by saying this: “Mankind is a single human body, and each nation a part of that body. We must never say “what does it matter to me if some part of the world is ailing?” If there is such an illness, we must concern ourselves with it as though we were having that illness.” [1]

Dear Guests,

It is also a fact that there are some vexing difficulties in maintaining international cooperation, which is a must for success in the fight against terrorism. The most significant of these is the variety of international perceptions of terror and terrorism.

Another difficulty is the support which terrorism receives for various reasons, either openly or in secret. Terrorist organizations cannot survive without external support. To wage an international, armed, common, and determined struggle against terrorism, it is a sine qua non that, rising above any difference of interests, we cut off all support for terrorism.

Another general difficulty in international cooperation is the implementation of legal measures for countering terrorism. Numerous decisions have been taken, and related measures have been anticipated in the context of these decisions.

For instance, there are a great many resolutions of the United Nations Security Council concerning defence against terrorism. In particular, Resolutions 1368 and 1373 make the participation of all states in the fight against terrorism and cutting off support for terrorism obligatory. [2]

[1] Atatürk, 20 March 1937, (Atatürk’ün Fikir ve Düşünceleri, Hazırlayan Utkan Kocatürk, Atatürk Araştırma Merkezi Yay., Ankara, 1999, p. 385).

[2] In line with United Nations Security Council Resolution 1373 (28 September 2001), echoing Resolution 1368 (12 September 2001), states have the right to individual or collective self-defence against terrorist attacks. All states shall prevent and suppress the financing of terrorist acts, criminalise such acts, freeze financial assets or economic resources related to terrorism and elements as such, and prohibit activities related to the commission of such acts. In addition, states shall refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists.

On 25 March 2004 the European Union published its Anti-Terrorist Declaration, and on 30 November 2005 the Council of the European Union put forth its commitments in its Counter-Terrorism Strategy.[3]

Similarly, the 1999 NATO Strategic Concept defined terrorism as a crucial threat to security. At the 2002 Prague Summit, heads of state and government of NATO members reaffirmed their determined opposition to all kinds of threats, including terrorist activities. Furthermore, at the 2006 Riga Summit, the Alliance underlined terrorism's status as the chief threat facing it, and resolved to eliminate terrorism within 10 to 15 years.

However the attitude made clear in these decisions and declarations has unfortunately not been translated into practice at the desired level, and we can easily see a range of differences in application. This shortcoming not only weakens the rule of law but also has a negative impact on long-term international peace and security.

It is of great importance to adopt the decisions taken by NATO, the United Nations and the European Union within countries' domestic laws and policies.

Esteemed Guests,

During the symposium, the significance of international cooperation in the fight against terrorism in various areas was made clear by distinguished speakers. I fully agree with them, and I would like to emphasize that the highest area of cooperation is intelligence, and especially the timely sharing of accurate intelligence.

Intelligence activities to counter terrorism are different from standard intelligence activities. Intelligence in the defence against terrorism is performed in an uncertain environment and broader context ranging from nuclear weapons and illegal smuggling to suicide bombing and assassination.

Beside intelligence through technological means, human intelligence activities should be necessarily done concerning intelligence in the defence against terrorism. The first and most important action in maintaining global cooperation to effectively counter globalised terrorism is timely intelligence-sharing among national and international intelligence organizations.

[3] The Council of the European Union, The European Union Counter-Terrorism Strategy, paragraphs 6, 8, 28 and 29, and European Union Strategic Objectives for Combating Terrorism (Annex 1 to the Declaration on Combating Terrorism).

Distinguished Guests,

It is well known that aside from their benefit to human life, technological advances can easily be exploited for malicious ends, and this may cause serious problems.

Recent technological leaps in means of communication and transportation in particular and their increasingly usage by terrorists have created an environment that is ripe for terrorism to be globalized.

By exploiting these technological advances, terrorist organizations can more easily communicate with each other and maintain the funding they need to continue.

Terrorist organizations, by using means of communication, especially cyberspace, for their own purposes, gather information for their planned actions, work to train their members, ensure financial support, and spread propaganda by creating fear and panic among target populations, and twist information to their corrupted ends in order to sway public opinion.

The main purpose of terrorist organizations is to convey their messages to the public via violence. Hence, the media bears a great responsibility in averting the fear and panic that terrorism tries to sow among the public.

Cyber-terrorist attacks, by causing large-scale economic and human losses, can create fear and panic at the target populations, just as with traditional terrorist attacks. Owing to this, cyber-terrorist attacks against computer networks used in critical infrastructure are threats to security.[4]

Within this context, especially it is critical to raise the consciousness of Internet users, take protective physical and technological measures, adapt legal arrangements to the conditions created by cyberspace, and coordinate the work by institutions created for this purpose at the national and international levels.

Dear Guests,

As stated by the distinguished speakers, the proper use of strategic communication, which is a two-way communication, has significant effects in countering terrorism. Success in strategic communication depends on achieving the desired changes in the attitudes of the target population by conveying the purpose, necessity, and methods for countering terrorism through the right

[4] Denning, D.E., “Is Cyber Terrorism Coming? The George C. Marshall Institute, Mayıs 2, 2002.

messages. However, the messages conveyed and existing policies should be mutually supportive and in harmony.

Distinguished Guests,

From the very beginning Turkey has contributed to counter-terrorism efforts in the United Nations and NATO, and has signed 12 international conventions on preventing terrorism. Furthermore, by establishing the Centre of Excellence-Defence Against Terrorism in line with decisions taken at the 2002 NATO Prague Summit, it institutionalized its contributions.

During its current non-permanent membership on the UN Security Council, Turkey has prioritized sharing its experiences in the fight against terrorism with the United Nations. Turkey continues to display its determination through its contributions to the UN Counter-Terrorism Committee and by providing strong support to Security Council decisions on combating terrorism.

Turkey believes that terrorism constitutes the greatest challenge to human rights and international peace and security. Turkey condemns all terrorist activities without any distinction, whether they are religious, ideological, ethnic, or regional.

Ecosystem, which is emphasized by the Chief of Turkish General Staff in his opening remarks, is a phenomenon to be taken into consideration in defence against terrorism. It is clear that terrorism is a part of this ecosystem which surrounds and makes it possible to survive. Thus, people, who fight against terrorism, have also responsibility of defending against this system.

Countering terrorism is a long-term process. We cannot find solutions to everything in a single symposium. I sincerely hope that the results of our Third Symposium on Global Terrorism and International Cooperation help us to overcome the difficulties in international cooperation that I have mentioned here.

It is highly probable for terrorism, including cyber terrorism, to take place among threats and risks targeting Security in the New Strategic Concept of NATO which is still worked on by 12 Eminent Persons and will probably be presented to the Secretary General of NATO next month.

Our intention is to convey the outcomes of this symposium to the group of these Eminent Persons if we can manage. I believe that the viewpoints shared and the results obtained will really contribute to the working of NATO at least.

Distinguished Guests,

In the presence of you all, I would like to thank the distinguished members of the Centre of Excellence-Defence Against Terrorism, who have strived hard to organize and achieve this Symposium, which has brought you together, our esteemed guests, who are committed to the continuation of international cooperation in the fight against terrorism, which carries so much importance.

I would also like to thank all of the distinguished participants, the academics, scholars and experts who shared their views, knowledge and experience with us by presenting their papers.

Of course, apart from what we see as we sat in our chairs or up here on the stage, many anonymous heroes have worked behind the curtains for the success of the Symposium. I would like to thank everyone in the name of Turkish General Staff, myself and yourself with your permission ranging from security forces who have maintained a secure environment for the success of the organization and translators who worked patiently in their cabins to press members who tried to pursue all of the organization.

In concluding my speech, I will be presenting the distinguished guests with their plaques.

I would also like to offer you my best regards and wishes for a good journey back.

Thank you.